

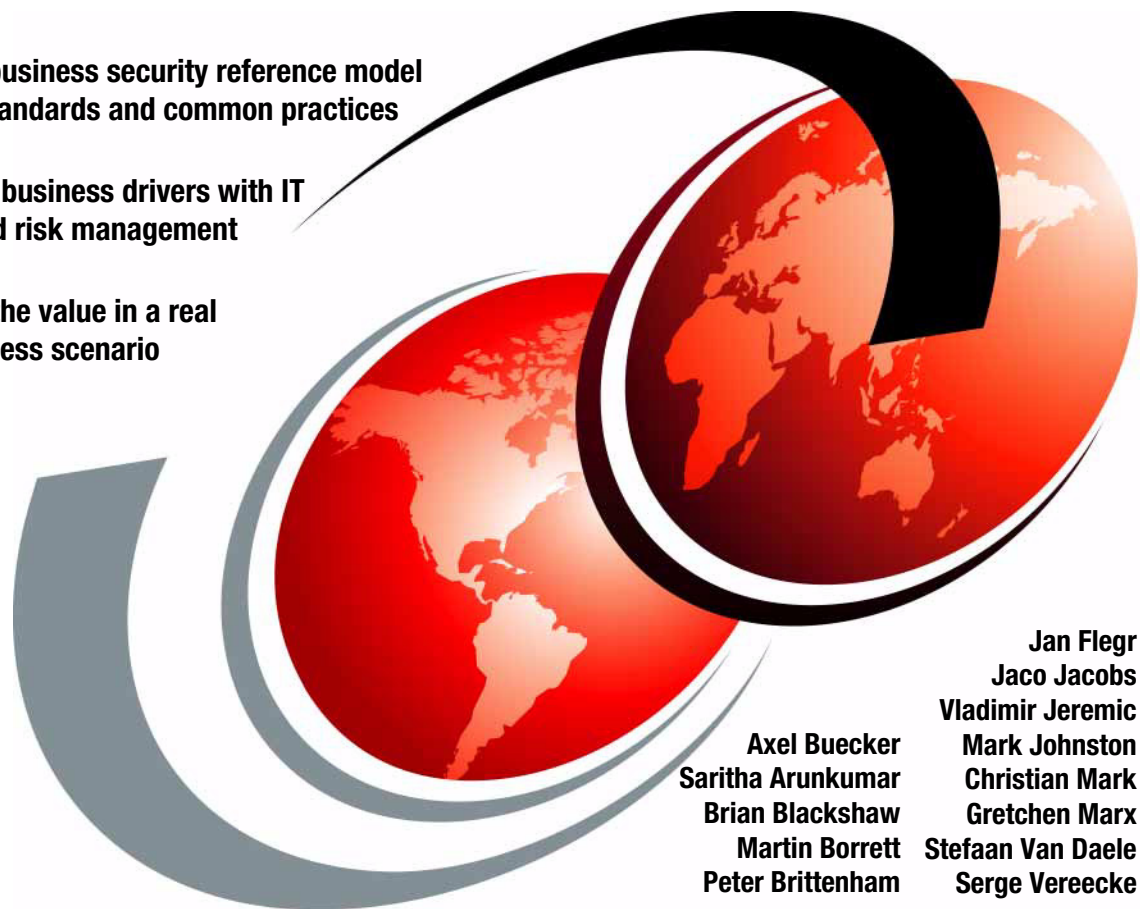


# Using the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security

Building a business security reference model based on standards and common practices

Connecting business drivers with IT security and risk management

Explaining the value in a real world business scenario



Jan Flegr  
Jaco Jacobs  
Vladimir Jeremic  
Mark Johnston  
Christian Mark  
Gretchen Marx  
Stefaan Van Daele  
Serge Vereecke  
Axel Buecker  
Saritha Arunkumar  
Brian Blackshaw  
Martin Borrett  
Peter Brittenham





International Technical Support Organization

**Using the IBM Security Framework and IBM Security  
Blueprint to Realize Business-Driven Security**

April 2013

**Note:** Before using this information and the product it supports, read the information in “Notices” on page vii.

**Third Edition (April 2013)**

**© Copyright International Business Machines Corporation 2013. All rights reserved.**

Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.



# Contents

<b>Notices</b> .....	vii
Trademarks .....	viii
<b>Foreword</b> .....	ix
Preface .....	x
The team who wrote this book .....	xii
Now you can become a published author, too! .....	xv
Comments welcome .....	xvi
Stay connected to IBM Redbooks .....	xvi
<b>Summary of changes</b> .....	xvii
April 2013 (previous editions published in Redpaper format) .....	xvii
<b>Chapter 1. Introducing the IBM Security Framework and IBM Security Blueprint</b> .....	1
1.1 Business context for IT security .....	2
1.2 Drivers that influence security .....	2
1.2.1 Business drivers that influence security .....	3
1.2.2 IT drivers that influence security .....	5
1.3 Common industry approaches to IT security management .....	7
1.4 IBM Security Framework .....	8
1.4.1 Advanced Security and Threat Research .....	10
1.4.2 People .....	11
1.4.3 Data .....	13
1.4.4 Applications .....	15
1.4.5 Infrastructure .....	17
1.4.6 Security Intelligence and Analytics .....	18
1.4.7 Security maturity model .....	20
1.5 IBM Security Blueprint .....	21
1.5.1 Foundational Security Management .....	23
1.5.2 Security Services and Infrastructure .....	26
1.5.3 Architectural principles .....	27
<b>Chapter 2. The components of the IBM Security Blueprint</b> .....	31
2.1 Foundational Security Management .....	32
2.2 Subcomponents .....	34
2.2.1 Command and Control Management .....	34
2.2.2 Security Policy Management .....	39
2.2.3 Risk and Compliance Assessment .....	46

2.2.4 Identity, Access, and Entitlement Management . . . . .	58
2.2.5 Data and Information Protection Management . . . . .	67
2.2.6 Software, System, and Service Assurance . . . . .	78
2.2.7 Threat and Vulnerability Management . . . . .	86
2.2.8 IT Service Management . . . . .	95
2.2.9 Physical Asset Management . . . . .	100
2.3 Conclusion. . . . .	104
<b>Chapter 3. IT security frameworks and standards . . . . .</b>	<b>105</b>
3.1 Industry information security and privacy standards profile model . . . . .	106
3.2 TOGAF . . . . .	108
3.2.1 What is architecture in the context of TOGAF. . . . .	108
3.2.2 Architecture types that are supported by TOGAF . . . . .	110
3.2.3 Industry guidance and techniques . . . . .	111
3.2.4 IBM Security Blueprint mapping . . . . .	115
3.3 IBM Unified Method Framework . . . . .	115
3.3.1 Industry guidance and techniques . . . . .	117
3.3.2 IBM Security Blueprint mapping . . . . .	119
3.4 Sherwood Applied Business Security Architecture . . . . .	120
3.4.1 Common strategy and terminology . . . . .	121
3.4.2 Industry guidance and techniques . . . . .	122
3.4.3 IBM Security Blueprint mapping . . . . .	126
3.5 Control Objectives for Information and Related Technology. . . . .	126
3.5.1 COBIT 4.1 . . . . .	129
3.5.2 COBIT 5 . . . . .	131
3.5.3 Maturity model and assessment using COBIT . . . . .	133
3.5.4 IBM capability mapping . . . . .	133
3.6 ISO/IEC 27002:2005 . . . . .	134
3.6.1 IBM Security Blueprint mapping . . . . .	135
3.7 Payment Card Industry Data Security Standard . . . . .	136
3.7.1 IBM Security Blueprint mapping . . . . .	136
3.8 Sarbanes-Oxley Act . . . . .	136
3.8.1 Common strategy and terminology . . . . .	137
3.8.2 Industry guidance and techniques . . . . .	137
3.8.3 IBM capability mapping . . . . .	138
3.9 Health Insurance Portability and Accountability Act . . . . .	139
3.9.1 Common strategy and terminology . . . . .	140
3.9.2 Industry guidance and techniques . . . . .	140
3.9.3 IBM capability mapping . . . . .	142
3.10 Conclusion. . . . .	143
<b>Chapter 4. Using O-ESA to develop an enterprise security architecture</b>	<b>145</b>
4.1 Introduction to O-ESA . . . . .	146

4.2 Alignment of the IBM Security Blueprint and O-ESA. . . . .	149
4.3 O-ESA based approach to develop an enterprise security architecture .	157
4.3.1 Introduction . . . . .	157
4.3.2 Governance. . . . .	160
4.3.3 Architecture . . . . .	162
4.3.4 Operations. . . . .	169
4.4 Conclusion. . . . .	175
<b>Chapter 5. Business scenario for the Mobile Device Security solution</b>	
<b>pattern . . . . .</b>	<b>177</b>
5.1 Company overview . . . . .	178
5.2 Business vision . . . . .	180
5.3 Business requirements . . . . .	181
5.3.1 IBM Security Framework mapping to business requirements. . . . .	182
5.4 Security requirements . . . . .	184
5.4.1 IBM Security Blueprint mapping to security requirements . . . . .	185
5.5 Security architecture . . . . .	191
5.5.1 Gathering requirements . . . . .	192
5.5.2 Defining strategy, planning, and policies from the requirements (program management and governance) . . . . .	195
5.5.3 Defining security domains (logical architecture) . . . . .	197
5.5.4 Defining security services placement in the security domains . . . .	198
5.5.5 Defining a component model for the security services (logical architecture) . . . . .	201
5.5.6 Use case . . . . .	201
5.5.7 Operational model. . . . .	204
5.5.8 Defining security operations for the concerned security services . .	207
5.6 Conclusion. . . . .	208
<b>Related publications . . . . .</b>	<b>211</b>
IBM Redbooks . . . . .	211
Other publications . . . . .	211
Online resources . . . . .	212
Help from IBM . . . . .	216



# Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

*IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.*

**The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:** INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

## **COPYRIGHT LICENSE:**

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

# Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at <http://www.ibm.com/legal/copytrade.shtml>

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:


IBM®

Rational®

Redbooks®

Redguide™

Redpaper™

Redbooks (logo) ®

Tivoli®

The following terms are trademarks of other companies:

ITIL is a registered trademark, and a registered community trademark of The Minister for the Cabinet Office, and is registered in the U.S. Patent and Trademark Office.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

# Foreword

As the custodian of the IBM® Security Blueprint and sponsor of this initiative, I am delighted to introduce this latest edition of the IBM Security Blueprint. It follows from the tremendous success of and interest from clients around the world in the second edition, which was downloaded more than 21,000 times. It is used by many clients and their security professionals. The need for a structured and well-founded approach to security capabilities is something our clients tell me that is vital in this era of cyber threats and rigorous regulation.

The initial idea for this third version of the IBM Security Blueprint started during informal discussions with clients and colleagues at the IBM Pulse international conference in Las Vegas during March 2012. I remember during an early breakfast meeting in Brussels between Stefaan Van Daele and myself, discussing the scope of the possible areas for both improvement and more content. This discussion ultimately resulted in the building of an international team with broad experience in many different security domains and team members that contributed from all over the world.

This updated version represents a significant step forward in describing and explaining the IBM Security Blueprint approach. There is more detail, use cases, and insight into other industry frameworks. I am proud of the result of this collaboration and I must say that such efforts rely on the passion and commitment of a number of IBMers, and this version is no exception. I want to say a big thank you to the team, and in particular thanks to Axel Buecker for keeping this project on track with his extensive publishing experience and great work on security at the International Technical Support Organization.

Martin Borrett  
Director of the IBM Institute for Advanced Security  
Europe

# Preface

Security is a major consideration in the way that business and information technology systems are designed, built, operated, and managed. The need to be able to integrate security into those systems and the discussions with business functions and operations exists more than ever.

This IBM Redbooks® publication explores concerns that characterize security requirements of, and threats to, business and information technology (IT) systems. This book identifies many business drivers that illustrate these concerns, including managing risk and cost, and compliance to business policies and external regulations. This book shows how these drivers can be translated into capabilities and security needs that can be represented in frameworks, such as the IBM Security Blueprint, to better enable enterprise security.

Over the last few decades, industry groups and standards bodies developed frameworks that serve as a baseline for certain aspects of security, and this book describes many of these frameworks in some detail.



To help organizations with their security challenges, IBM created a bridge to address the communication gap between the business and technical perspectives of security to enable simplification of thought and process. As depicted in Figure 1, the IBM Security Framework can help you translate the business view, and the IBM Security Blueprint describes the technology landscape view. Together, they can help bring together the experiences that we gained from working with many clients to build a comprehensive view of security capabilities and needs.

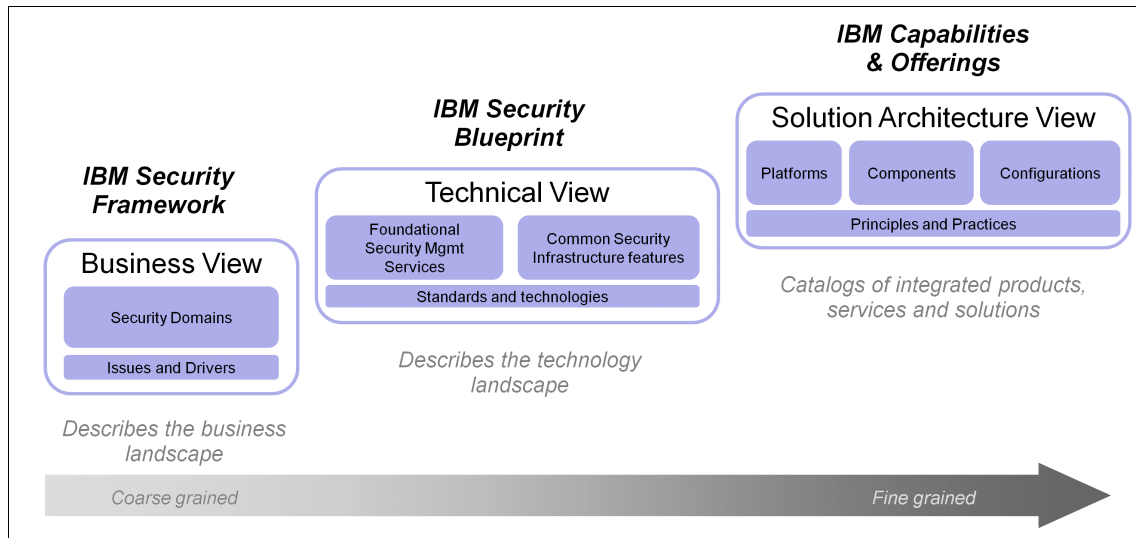


Figure 1 Positioning the IBM Security Framework and IBM Security Blueprint

The IBM Security Framework divides Information Security into the following areas of concern (or domains):

- ▶ Governance, Risk Management, and Compliance
- ▶ Advanced Security and Threat Research
- ▶ People
- ▶ Data
- ▶ Applications
- ▶ Infrastructure
- ▶ Security Intelligence and Analytics

The IBM Security Blueprint expands on the business-oriented view of the IBM Security Framework by mapping the domains to a core set of security components that represent capabilities and services. Organizations can realize these capabilities through hardware (including appliances), software, and services. The IBM Security Blueprint aims to describe these security capabilities in vendor and product independent terms, using common and accepted industry definitions.

This book is intended to be a valuable resource for business leaders, security officers, and consultants who want to understand and implement enterprise security by considering a set of core security capabilities and services.

## The team who wrote this book

This book was produced by a team of specialists from around the world working at the International Technical Support Organization, Austin Center.

**Axel Buecker** is a Certified Consulting Software IT Specialist at the ITSO, Austin Center. He writes extensively and teaches IBM classes worldwide on areas of software security architecture and network computing technologies. He holds a degree in Computer Science from the University of Bremen, Germany. He has 25 years of experience in various areas that are related to workstation and systems management, network computing, and e-business solutions. Before he joined the ITSO in March 2000, Axel worked for IBM in Germany as a Senior IT Specialist in Software Security Architecture.

**Saritha Arunkumar** is a Senior Security Architect working in Emerging Technology Services, Hursley, United Kingdom. Saritha has 12+ years of experience in the IT Security space. She has deep expertise in Identity and Access Management solutions, Web Services security, public key Infrastructure, cryptography, and Internet security. Saritha has in-depth experience in defining end-to-end security architectures, high level and detail security designs, and infrastructure security solutions. Saritha has a Bachelor's degree in Engineering, an MBA in Operations Management, and is pursuing her Ph.D. in Mobile Security from City University, London.

**Brian Blackshaw** has over 15 years of experience in the area of data, network, and application security. He is a strategist on the IBM Security Systems strategy team. Brian joined IBM through the acquisition of Watchfire, an application security company, where he was Director of Product Management. Before Watchfire, he held security-centric positions at Cisco and McAfee.

**Martin Borrett** is the Director of the IBM Institute of Advanced Security in Europe. He leads the Institute and advises at the most senior level in clients on policy, business, technical, and architectural issues that are associated with security. Martin has led the IBM Security Blueprint work over the last two years. He is also co-author of *Understanding SOA Security Design and Implementation*, SG24-7310. He is Chairman of the European IBM Security User Group community and Chairman of the IBM UKI Technical Consulting Group. He is a member of the board of EOS, the European Organisation for Security. He is a Fellow of the British Computer Society, and a Chartered Engineer (CEng) and member of the IET.

**Peter Brittenham** has more than 30 years of experience in the IT industry. He is a Security Architect for IBM security solutions, which covers identity and access management, data privacy and protection, application security, and infrastructure security. Before this position, Peter was one of the lead architects for the IBM Trusted Identity Initiative, which was focused on bringing a new level of trust and confidence to identification systems, that is, how a person is enrolled in a system, how their identity credentials, are issued, how those credentials are used, and how those credentials are dispensed.

**Jan Fleg** is a Certified IT Specialist at the IBM Software Services in Praha, Czech Republic. He works on various local and international security services implementation projects across the EMEA region. He has a degree in Automated Systems Control from the Institute of Technology in Plzen, Czech Republic. He has 28 years of overall IT experience, including mainframe, UNIX, and workstations. Jan has been with IBM for 12 years, focusing mainly on IT security for the last six years.

**Jaco Jacobs** is a manager in the Accenture Technology Consulting group's Security Practice and has delivered various Information Security services to customers worldwide. He was responsible for developing and delivering information security education and contributed to the development of Security Services for an international client base. He is a Certified Information Systems Security Professional (CISSP) and holds numerous Information Security Certifications. He has been a practicing Information Security Professional since 1998 with extensive experience in Enterprise Security Architecture, Risk Management, Vulnerability Management, Compliance Management, Incident and Event Management, and Intrusion Management.

**Vladimir Jeremic** is a Security Enablement Specialist working on course development and delivery in IBM Security Center of Excellence, focusing on technical aspects of IBM products. Vladimir also worked for many years as a Certified Security Managing Consultant with the IBM Global Services team, where he focused on architecture and implementation of the IBM Security portfolio. He has over ten years of experience in the IT field that is related to security, networking, and programming. Vladimir is an IBM Tivoli® Certified Professional for several IBM security products and IBM Certified Consultant. He holds a Bachelor of Science degree in Electrical Engineering from the University of Novi Sad in Serbia. Vladimir has a passion in developing and sharing security knowledge and he contributed to several other IBM Redbooks publications.

**Mark Johnston** is a Security Solution Architect and part of the IBM Worldwide Security Tiger Team, Australia. Mark has over 12 years experience in the IT Industry. He has consulted with various federal and state government departments, helping them to build identity, access, and security monitoring solutions for their business. He has worked in a number of countries in Asia, Europe, and the US. Mark worked as a consultant in the IBM Security and Privacy consulting division and is developing security workshop offerings to assess the maturity of IT security controls in organizations today.

**Christian Mark** is a senior Information Security Architect with over 12 years of experience in technology and information security, and a background in most of the technologies that drive today's organizations. Christian is member of The Open Group Security Forum Steering Committee and holds various professional certifications and is specialized in security and risk management into enterprise-level architectures. He recently served several years as Lead Security Architect and trusted advisor for some IBM major financial customers in the European Strategic Outsourcing business.

**Gretchen Marx** is a Program Manager in the IBM Security Systems Division strategy group and is responsible for developing cross-portfolio strategies in areas such as Data Loss Prevention and big data. She has an MBA from the University of California at Berkeley and has written numerous college textbooks in the areas of computer applications and the Internet. Before she joined the IBM Security Systems Division in July 2011, Gretchen was a Corporate Strategy Consultant in the area of risk modeling, where she helped develop a patent-pending methodology, including risk taxonomy and statistical algorithms, to forecast integration risks with the IBM acquisition target.

**Stefaan Van Daele** is a Senior Security Architect in the IBM Security Tiger Team covering the EMEA region and assisting customers with the definition of solutions to their security requirements. Before he joined the Tiger Team in 2011, Stefaan was a Security Architect in IBM Services since 1997, where he was mostly involved in Identity and Access Management projects. As a student, Stefaan started his digital life on a Commodore 64 in the early eighties and his first job in 1988 was as a developer in C and Assembler. Now he focuses more on Enterprise Security Architectures.

**Serge Vereecke** is a Certified Security Architect in the IBM Security Services group. His role involves security architecture and solution design for projects that are based on the IBM Security product portfolio. His areas of expertise include system integration and information security that focuses on identity and access management, single sign-on, and cloud computing security. Serge has over 12 years of experience in the IT industry and holds a Ph.D. degree in Chemistry from K.U. Leuven, Belgium.

Thanks to the following people for their contributions to this project:

Emma Jacobs, Wade Wallace, Erica Wazewski  
**International Technical Support Organization, Austin Center**

Jeff Crume, Carsten Lorenz, Ivan Milman, Kevin Skapinetz, Frank Sommer,  
Jim Whitmore  
**IBM**

Thanks to the authors of the first and second edition of this IBM Redbooks publication, *Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security*, published in July 2009 and updated in December 2010:

David Crowther, Foulques de Valence, Guilherme Monteiro, Michel Oosterhof,  
Andrew Quap, Maria Schuett, Kai Stockmann, Carsten Lorenz, Calvin Powers,  
Martin Borrett

Thanks to the following people for their contributions to this project:

Nick Coleman, Ivan Milman, Jim Whitmore, and the whole IBM Security  
Architecture Board team  
**IBM**

## Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an ITSO residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at:

[ibm.com/redbooks/residencies.html](http://ibm.com/redbooks/residencies.html)

## Comments welcome

Your comments are important to us!

We want our books to be as helpful as possible. Send us your comments about this book or other IBM Redbooks publications in one of the following ways:

- ▶ Use the online **Contact us** review Redbooks form found at:  
[ibm.com/redbooks](http://ibm.com/redbooks)
- ▶ Send your comments in an email to:  
[redbooks@us.ibm.com](mailto:redbooks@us.ibm.com)
- ▶ Mail your comments to:  
IBM Corporation, International Technical Support Organization  
Dept. HYTD Mail Station P099  
2455 South Road  
Poughkeepsie, NY 12601-5400

## Stay connected to IBM Redbooks

- ▶ Find us on Facebook:  
<http://www.facebook.com/IBMRedbooks>
- ▶ Follow us on Twitter:  
<http://twitter.com/ibmredbooks>
- ▶ Look for us on LinkedIn:  
<http://www.linkedin.com/groups?home=&gid=2130806>
- ▶ Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:  
<https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm>
- ▶ Stay current on recent Redbooks publications with RSS Feeds:  
<http://www.redbooks.ibm.com/rss.html>

# Summary of changes

This section describes the changes that are made in this edition of the book and in previous editions. This edition might also include minor corrections and editorial changes that are not identified.

Although this book appears to be a first edition IBM Redbooks publication, indicated by the -00 extension in the document number, this book is actually the *third edition*. The previously available document was the IBM Redpaper™ publication *Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security*, REDP-4528. Because we extended our document substantially, we decided to publish it as a new book.

## April 2013 (previous editions published in Redpaper format)

This revision reflects the addition, deletion, or modification of new and changed information that is described below.

### New information

Here is information that is new in this edition:

- ▶ To better understand the diversity of different standards when you deal with IT security, we added Chapter 3, “IT security frameworks and standards” on page 105. This chapter provides an overview of some of the most common standards and frameworks and explains their relationship with the IBM Security Blueprint and IBM Security Framework.
- ▶ The IBM Security Blueprint can help you identify the necessary security services and related subcomponents to develop a security solution for your organization. But this identification is not enough to begin deploying software products, designing policies, or segregating your network. The next step can be the translation of what you learned into an Enterprise Security Architecture (ESA) to set the context and constraints for the technical design. In Chapter 4, “Using O-ESA to develop an enterprise security architecture” on page 145 leverages the *Open Enterprise Security Architecture (O-ESA)* from the Open Group (reference Catalog number G112, April 2011) to describe an approach on how an ESA can be created from the IBM Security Blueprint.

## Changed information

Here is information that is changed in this edition:

- ▶ We updated the IBM Security Framework information to reflect the changes that were introduced by the IBM Security Systems division. These changes also required a slight update to the IBM Security Blueprint representation. However, none of the Foundational Security Management components had to be changed. For more information, see Chapter 1, “Introducing the IBM Security Framework and IBM Security Blueprint” on page 1.
- ▶ In Chapter 2, “The components of the IBM Security Blueprint” on page 31, we extended the information for three of the Foundational Security Management subcomponents to now have a similar level of detail with the remaining subcomponents:
  - Security Policy Management
  - Data and Information Protection Management
  - Software, System, and Service Assurance
- ▶ Finally, we provide a new business scenario in Chapter 5, “Business scenario for the Mobile Device Security solution pattern” on page 177.





# Introducing the IBM Security Framework and IBM Security Blueprint

To provide some background and to set the scene for the IBM Security Framework and IBM Security Blueprint, this chapter starts with a description of the typical business context for information technology (IT) security. This chapter examines how business leaders can use security, risk, and compliance-related investments to competitively position their organizations and satisfy complex regulatory requirements. The remainder of this chapter is dedicated to introducing the IBM Security Framework and the IBM Security Blueprint.

This chapter includes the following sections:

- ▶ Business context for IT security
- ▶ Drivers that influence security
- ▶ Common industry approaches to IT security management
- ▶ IBM Security Framework
- ▶ IBM Security Blueprint

## 1.1 Business context for IT security

Organizations rely on Information Security (IS) systems more than ever to detect threats to intellectual property, reputation, and privacy. Organizations often adopt a piecemeal or technology-driven approach to security. Using this approach alone does not provide sufficient protection for business processes and assets against these business risks, as it might overlook key, cross-discipline aspects.

As the pace of globalization continues and new technologies emerge, traditional boundaries between organizations continue to disappear. The ideal response involves planning and assessment to identify risks across key business areas, including people, processes, data, and technology throughout the entire organization. It is important to take a holistic approach that can facilitate a business-driven security blueprint and strategy that can act as an effective defense for the entire organization.

Organizations should build business services that are *secure by design*, meaning that security is intrinsic to their business processes, product development, and daily operations. Security should be factored into the initial design, not bolted on afterward. This approach enables an organization to securely and safely adopt new forms of technology, such as cloud computing and mobile device management, and business models, such as teleworking and outsourcing, can be more safely used for cost benefit, innovation, and shorter time to market.

With these security domains, capabilities, and services as a backdrop, this first section covers a detailed overview of the IBM Security Framework, the IBM Security Blueprint, and the IBM Security Maturity Model. The later sections explain the IBM Security Blueprint in more detail by describing its components and subcomponents.

## 1.2 Drivers that influence security

Most projects include both business and IT drivers, with business drivers generally being the initiating factor. Here is a closer look at these influencing factors:

- Business drivers

Business drivers measure value, risk, and economic costs that influence an organization's approach to IT security. Value drivers determine the worth of assets of the system to the business and of the business itself. Risk drivers involve compliance, corporate structure, corporate image, and the risk tolerance of the company. Economic drivers determine productivity impact, competitive advantage, and system cost.

Business drivers also represent issues and consequences of significance to the stakeholders of the managed business system. This set of drivers might vary from industry to industry, from organization to organization in the same industry, and even from different business applications within an organization.

► IT drivers

IT drivers represent operational constraints in the general IT environment. For example, the complexity of a system, including its environment, that is exposed to internal and external threats presents risks that the organization must address. The IT drivers represent technical considerations that can affect the trustworthiness of the IT environment and the managed business systems as a whole. IT drivers are universal and must be considered within the context of the business drivers in all efforts. The combination of business and IT drivers represents the key initiatives for security management.

## 1.2.1 Business drivers that influence security

Business drivers represent a relationship between the IT organization and the rest of the business. They refer to business needs that must be supported by the IT security infrastructure.

### **Correct and reliable operation**

Correct and reliable operation is the degree to which the business must be accurate and consistent in its operation. Correct operation means that the operations perform the correct response or function with no errors. Reliable means that the same result occurs all the time. Any IT system must consistently provide stakeholders with the expected results.

Security events and incidents might impact the correct and reliable operation of these business processes. They might also affect the underlying IT infrastructure or upstream and downstream business processes. The consequences of a defective service (incorrect or varying results over time) might be significant to the consumer of the service, and therefore to the provider of the service.

### **Service-level agreements**

This driver applies to circumstances where security threats and threat agents can impact an organization's ability to conduct business. Service-level agreements (SLAs) incorporate acceptable conditions of operation within an organization. SLAs might vary from business system to business system or application to application. Availability of systems, data, and processes are conditions that are commonly referenced within SLAs.

## **IT asset value**

From a business perspective, the IT asset value is directly related to the value of the business transactions that it supports. These assets might be tangible or intangible. For an e-retailer, these assets are tangible. For a financial services company, the asset might be client information or other data that is used in transactions.

## **Protection of the business asset value or brand image**

This driver captures the firm's desire to protect its image. The loss of goodwill from a security incident or attack has a direct consequence to the business. Therefore, the security measures should be proportional to the consequence. If an organization is confronted with a security breach, the desire to avoid negative publicity generally increases and the stipulation for this driver becomes stronger.

## **Legal and regulatory compliance**

Legal and regulatory compliance involves externally imposed conditions on the transactions in the business system and the company. This compliance includes the rules and policies that are imposed by industry, regulatory, and government organizations. Civil liability and criminal or regulatory penalties from a security incident or attack have a negative consequence on the business. Therefore, the extent of regulation and measures taken to ensure that compliance should be factored in this driver, including privacy issues, the ability to identify and document transactions and their initiators, and proving compliance.

## **Contractual obligation**

Security measures for an IT system should be proportional to the consequences incurred when the business encounters contractual liability from a security attack. For example, when security incidents occur, the business might be unable to fulfill its contractual obligations of providing goods or services.

## **Financial loss and liability**

Direct or indirect financial loss is a consequence to the business as a result of a security incident. Direct loss might include theft of assets, theft of service, or fraud. Indirect loss might include a loss that is based on civil or criminal judgment, loss of good will, impact to organizational reputation or brand image, or reprioritized budget allocation. This driver identifies the fact that security measures for an IT system are likely to be in proportion to these consequences.

## **Critical infrastructure**

This driver applies where security threats or threat agents can have a major impact on services or resources that are common to, or shared among, a community of businesses, the population at large, or both. Examples include telecommunications, electrical power grids, transportation systems, computing networks, and others. The loss of a critical infrastructure by its provider might have a ripple effect, causing secondary losses and driving security decisions for those parties that are affected. An important part of risk analysis is identifying critical infrastructure.

## **Safety and survival**

This driver applies where security threats and threat agents can have a major impact on aspects of human life, government function, and socio-economic systems. Examples of processes to be considered for safety and survival impact include continuity of critical infrastructure, medical systems, life support, or other high-impact or time-dependent processes.

### **1.2.2 IT drivers that influence security**

IT drivers comprise the second group of key security initiatives. These drivers are considered universal drivers that must be considered in every modern IT solution in a manner that is commensurate with the risks and consequences of a related failure or incident.

#### **Internal threats**

Security-related failures and incidents are caused by threats that are found within the physical and logical boundaries of the organization that operates and controls the IT system. These threats might be associated with technology or people.

An example of an internal threat is a poorly designed system that does not have the appropriate controls or a person who uses his ability to access the IT system or influence business or management processes to carry out a malicious activity.

#### **External threats**

Security-related failures and incidents are caused by threats that are found outside the physical and logical boundaries of the organization that operates and controls the IT system. These threats are also associated with technology or people. They seek to either penetrate the logical or physical boundary, or to influence business or management processes from outside the logical or physical boundary.

Examples of external threats are a computer virus or worm that penetrates the physical or logical network boundary. Another example is an attacker, or someone who gained the ability to act as an insider, using personal electronic credentials or identifying information.

### **IT service management commitments**

This driver identifies the fact that failure to manage the operation of the IT system might result in security exposures to the business. This driver can be divided into two categories, IT service delivery and IT service support.

- ▶ **Service delivery commitments**

The failure of the IT system can result in a security exposure to both business or management processes.

An example of security exposure for service delivery occurs when IT operational processes cannot respond to critical events in a timely manner. Another example would be IT resilience processes that cannot recover from a denial-of-service attack in a timely manner, resulting in a loss of capacity or response time for business processes.

- ▶ **Service support commitments**

The failure of the business or IT management system to meet its service-level agreements can be viewed as a security exposure to business or management processes.

An example of security exposure for service support is a situation in which the customer relationship processes do not add, modify, or remove users from access control lists in a timely manner.

### **IT environment complexity**

The complexity of the IT environment might contribute to the security or insecurity of the IT system. The IT environment reflects the infrastructure on which the business system is placed. For example, any IT environment that is connected to the intranet or extranet is exposed to internal or external threats or threat agents and requires specific security responses. A stand-alone facility represents the lowest complexity. A hosting facility with other systems and other firms represents a more complex environment. An environment with a larger number of systems, varied network access paths, or a complex architecture increases the complexity of an IT environment.

### **Business environment complexity**

Most business environments consist of an interconnected set of organizations, each with its own complex IT environment, business processes, and IT management processes. This complexity contributes to the risk associated with the IT system.

## Audit and traceability

This driver identifies the need for the IT system to support an audit of information that is contained within the system, whether it is associated with management data or business data.

## IT vulnerabilities

IT systems can contain vulnerabilities that are caused by many factors. They can occur because of mis-configuration of a system itself, or because of software defects. Many vulnerabilities can go undetected for long periods of time. They can lead to so called *zero day attacks* when they are discovered and rapidly exploited. Usually, it is this discovery or *disclosure* that leads to the actual exploitation, which results in the actual threat and risk to an organization. Exploitation might also be because of the usage of a function within a system in an unintended way that compromises the system or underlying data.

# 1.3 Common industry approaches to IT security management

IT security management is the term that is used for the set of management activities that are intended to address the business and technical issues described earlier in accordance with the resilience and risk management objectives for the managed business system.

The business drivers that are described in 1.2.1, “Business drivers that influence security” on page 3 have led to an increasing number of organizations that are adopting internationally accepted frameworks and preferred practices to help implement IT governance in their organization. Control Objectives for Information and related Technology<sup>1</sup> (COBIT), the International Organization for Standardization 27002:2005<sup>2</sup> (ISO/IEC 27002:2005), and the Information Technology Infrastructure Library<sup>3</sup> (ITIL) have emerged worldwide as some of the most respected frameworks for IT governance and compliance. For a closer look at these and other standards, see Chapter 3, “IT security frameworks and standards” on page 105.

---

<sup>1</sup> For more information about COBIT, go to <http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981>.

<sup>2</sup> To purchase a copy of ISO/IEC 27002:2005, go to [http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=50297](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297).

<sup>3</sup> For more information about ITIL, go to <http://www.itil-officialsite.com/home/home.asp>.

## 1.4 IBM Security Framework

Today, any business initiative inside an organization is guided by the principles of *Governance, Risk, and Compliance*, which are often seen as broad terms that typically have different meanings to different stakeholders across an organization. Each CxO is trying to manage risk for their domain and, therefore, have different priorities and points of view when it comes to handling these risks:

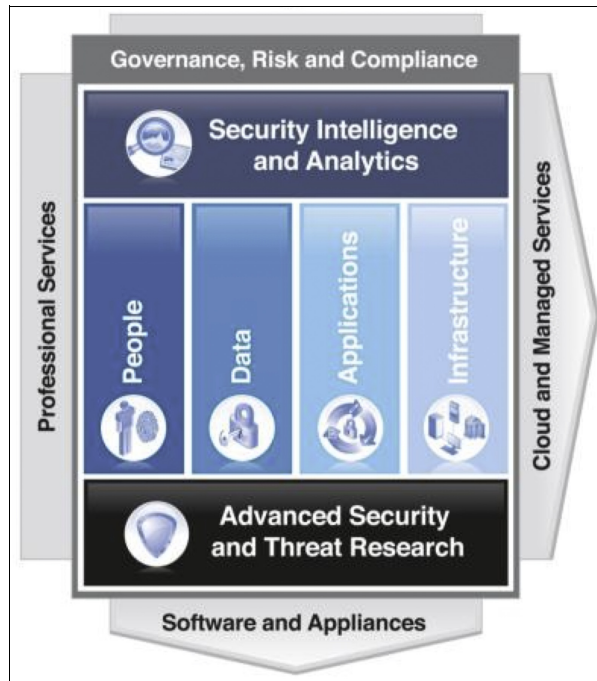
- CRO**      The *Chief Risk Officer* looks at the organization's overall risk profile and where they are most vulnerable to unexpected loss.
- CFO**      The *Chief Financial Officer* must ensure that the necessary controls are in place to have accurate financial statements.
- CISO**      The *Chief Information Security Officer* must ensure that the IT Infrastructure supports the overall business drivers of the organization. The CISO must minimize the risk of the IT environment and assess and communicate the impact of this environment on the overall organization from a Governance, Risk, and Compliance perspective.

Regardless of the organizational perspective of risk management, both process and IT controls must be established i to get a complete picture of the organization's *risk posture*. Establishing IT security controls, monitoring these controls, mitigating the risk observed through those controls, and reporting and communicating risk posture are critical capabilities for an IT security organization.

IBM created the IBM Security Framework to help ensure that every necessary IT security aspect can be properly addressed when you use a holistic approach to business-driven security.



The IBM Security Framework is depicted in Figure 1-1.



*Figure 1-1 The IBM Security Framework*

The capabilities that are described by the IBM Security Framework are based on a foundation of Advanced Security and Threat Research infrastructure. The solutions that are provided within the security domains and additional layers can be delivered through software, hardware (including appliances), and as services, whether managed, professional, or cloud based.

IBM provides the full breadth and depth of solutions and services that can enable organizations to take this business-driven, secure by design approach to security in alignment with the IBM Security Framework.

The following sections take a closer look into the layered model of the IBM Security Framework in the areas of:

- ▶ Advanced Security and Threat Research
- ▶ People
- ▶ Data
- ▶ Applications
- ▶ Infrastructure

- ▶ Security Intelligence and Analytics
- ▶ Security maturity model

### 1.4.1 Advanced Security and Threat Research

The threat landscape continues to evolve, and attacks continue to grow in number and complexity, as does the resulting business loss. It is critical to ensure that an advanced research team is being used to *stay ahead of the threat*. More than ever, ongoing research and development are imperative in ensuring that security solutions remain effective.

Advanced Security and Threat Research addresses the needs of the security market and can provide a foundation for understanding threats, their sources, and how to effectively respond to these attacks. Organizations are facing an explosion of data that must be incorporated into this research. For example, social media, custom malware, geo-location, advanced analytics, and the resulting targeted advanced persistent threats can dramatically increase the range and depth of the data that must be considered in Advanced Security and Threat Research.

It can be challenging for a typical organization to attempt to perform even a small portion of this overall research. There are many organizations that specialize in this type of research, including IBM.

These organizations research and monitor the latest Internet threat trends, develop security content for use in security products, and help advise organizations and the general public about how to respond to emerging and critical threats.

To be effective, such research groups can benefit from access to live customer data (for example, live monitoring of managed security services traffic). They need a global view where both global event monitoring and a global reach are important aspects. It is important to participate in industry consortiums and work with the appropriate government entities to stay ahead of the latest trends.

Figure 1-2 shows a summary and additional aspects to be addressed within the Advanced Security and Threat Research domain.

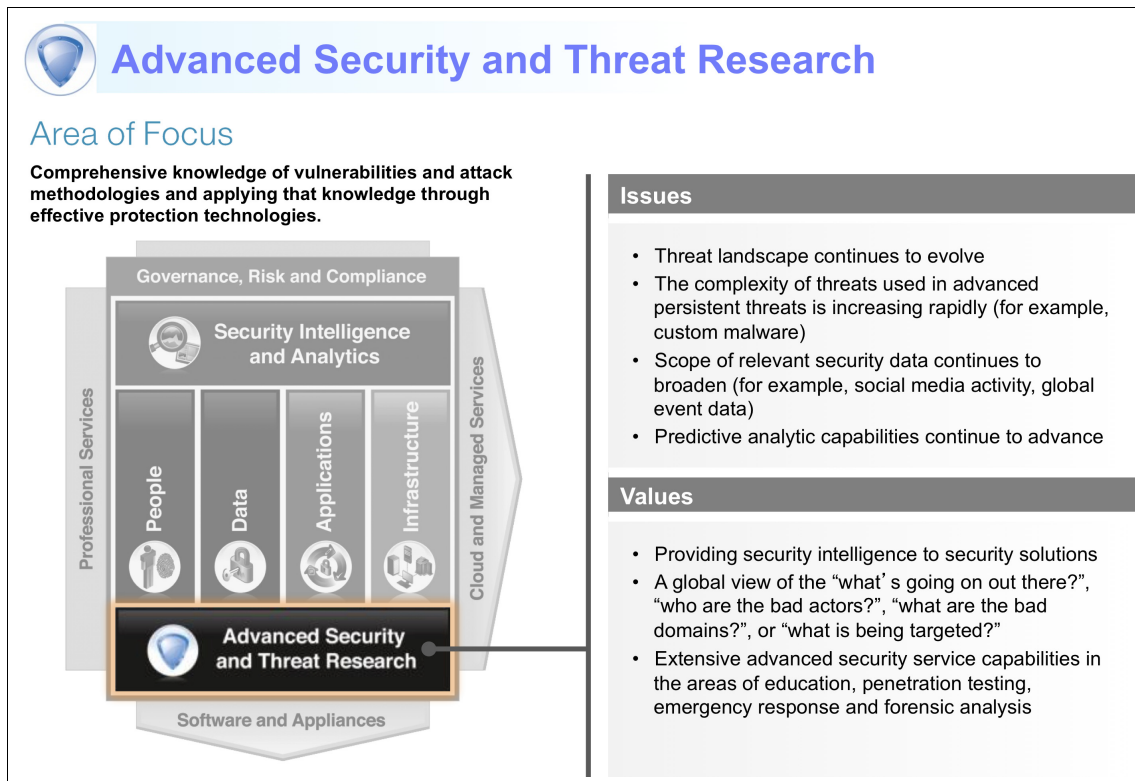


Figure 1-2 Advanced Security and Threat Research domain

## 1.4.2 People

Organizations must protect the assets and services that serve their business and support its operation. An important aspect of achieving this protection is provided through *identity management and access control*. Organizations register users and map them to identities or accounts. The relationships between people and the organization are expressed in terms of roles, rights, business policies, and rules. The ability to register people and describe their relationship within the organization is a key security enabler for other security domains.

Operationally, people that act in authorized roles in an organization, or as part of an extended relationship, are granted access to infrastructure, data, information, applications, and services. Concurrently, people that act in unauthorized roles or outside of the business policies and agreements are denied access to infrastructure, data, information, applications, and services.

Within an identity system, people can be issued a *credential* to prove their identity to IT systems. A credential can take any of several forms, including a physical identity card or logical token. The *trustworthiness* or *strength* of the credential is an important aspect of business policy and risk management. The ability to effectively manage the lifecycle of an identity, that is, the creation, removal, and role changes for dynamic populations of workforce, customer, or user communities, is important. The lifecycle of identities and credentials can be influenced by business cycles, employment cycles, and customer relationships, for example.

Often, identity systems must manage user roles, rights, and privileges across a heterogeneous environment that consists of multiple architectures and technology implementations within an IT infrastructure. Identity systems must be integrated with the appropriate sets of access controls. Especially in these complex situations, identity management systems can help mitigate the risk of dormant, expired, or shared IDs.

*Compliance* in an identity and access context is often externally motivated. For example, legislated privacy and evidence recording is a significant driver for the implementation of comprehensive user provisioning and identity-related record keeping.

Every organization must maintain privileged user access activity to ensure that no high-level access is being misused for malicious intent. In this context, it becomes more important to closely monitor privileged access and attribute every action to real people in the organization.

Figure 1-3 shows a summary and additional aspects to be addressed within the People domain.

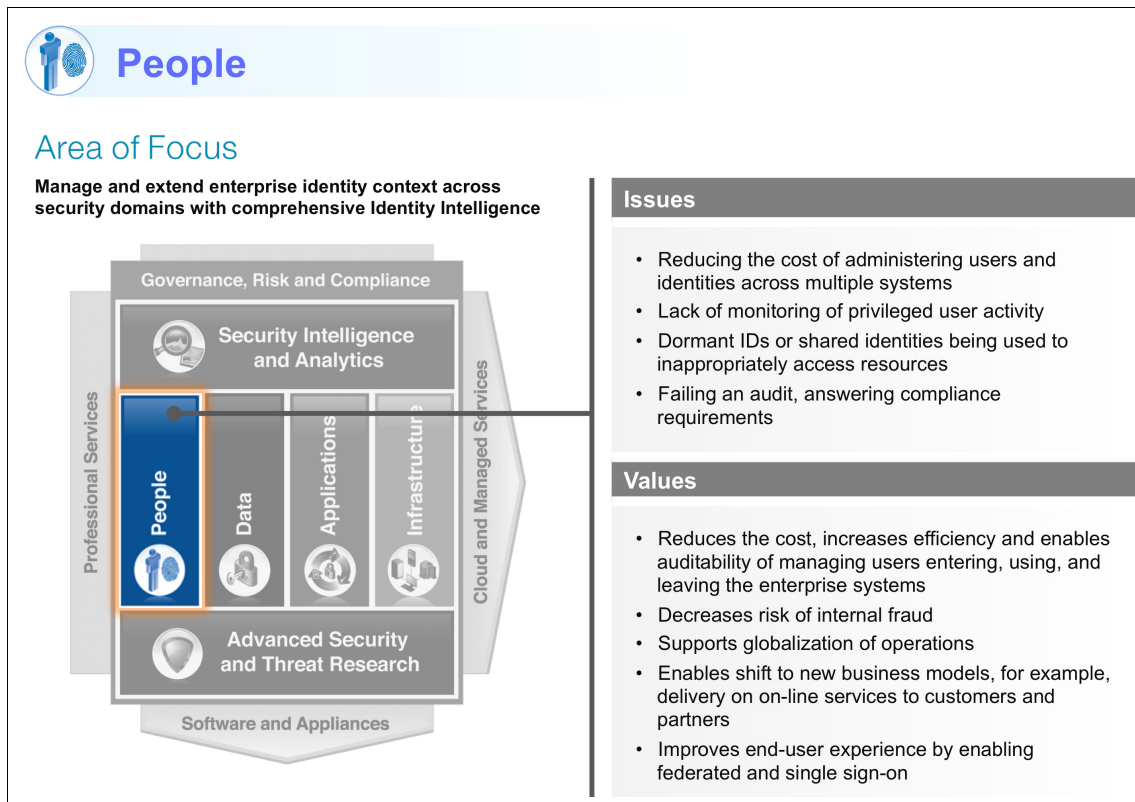


Figure 1-3 People domain

### 1.4.3 Data

Organizations must protect both the *raw data* and *contextualized information* that is within its span of control. The organization must provide guidance to IT about the classification and value of data and information, and how the risks to data and information must be managed. An effective plan for data and information protection includes maintaining a catalog or inventory of these assets, along with attributes, policies, enforcement mechanisms, and services that govern the access, transformation, movement, and disposition of data and information.

This data and information protection plan can be applied to business processes, business transactions, or business and infrastructure support processes. The protection of data and information covers the full information lifecycle, from creation to destruction across its various states, locations, and instantiations, as well as data that is stored (*at rest*) and data that is being physically or electronically transported (*in motion*).

The term *data* can be applied to a wide range of electronically encoded assets. These assets include software and firmware, which must be protected against technical risks (for example, to ensure that malicious code is not introduced) and business risks (to ensure that licensing terms are not violated). It also includes other types of intellectual property, such as plans and designs, and both structured and unstructured forms. Monitoring data access and protecting data from unwanted leakage or loss (*data loss prevention*) is made even more complex in today's changing environment of cloud delivery and mobile computing platforms.

Measuring and reporting on an organization's compliance regarding protection of data and information is a tangible metric of the effectiveness of the enterprise security plan. A *data and information compliance report* reflects the strength or weakness of controls, services, and mechanisms in all domains.

Figure 1-4 shows a summary and additional aspects to be addressed within the Data domain.

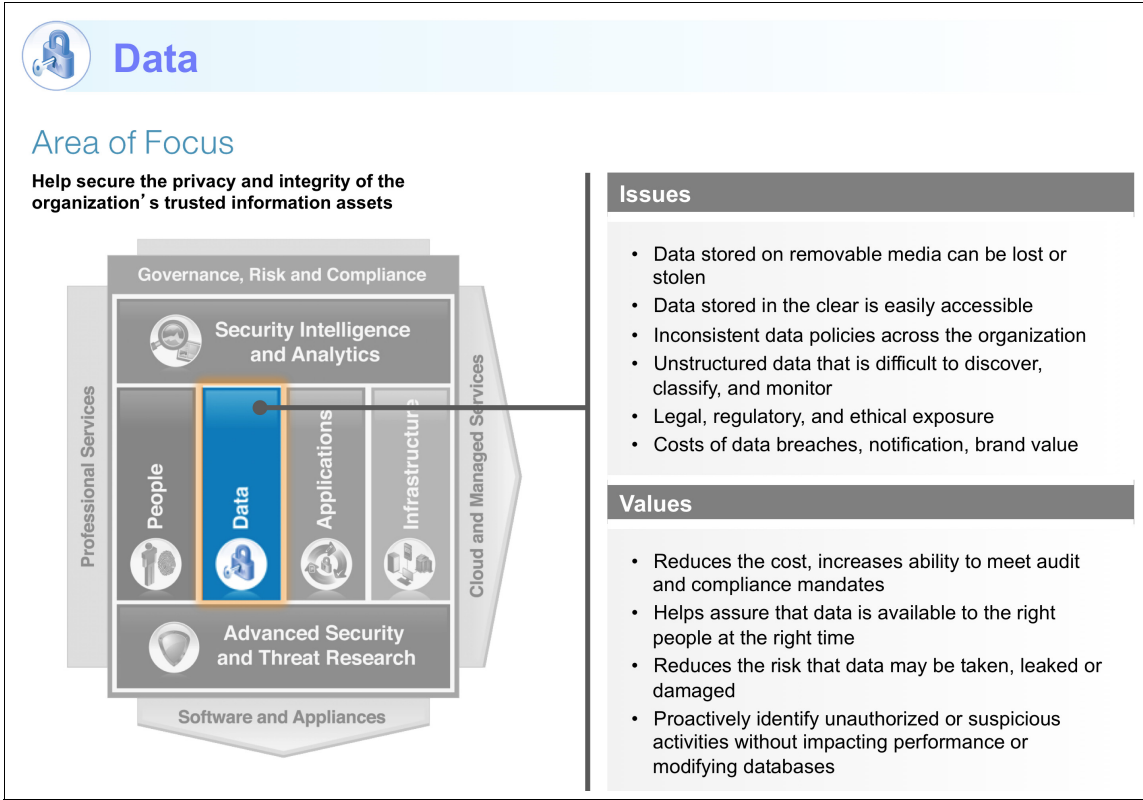


Figure 1-4 Data domain

### 1.4.4 Applications

It is imperative to have a layered approach to security that ensures that all security domains are appropriately addressed in an IT security infrastructure. One of the most effective ways to avoid a breach is to make sure that the applications your users are accessing are designed and implemented securely.

Organizations must proactively protect their *business-critical applications* from external and internal threats throughout their entire lifecycle, from design to development, test, and production. For example, whether an application is internally focused, such as a customer relationship management (CRM) system, or is an externally facing application, such as a new customer portal, clearly defined security policies and processes are critical to ensure that the application enables the business rather than introducing more risk.<sup>4</sup>

Automatic scanning of application source code, as well as vulnerability testing of operational systems, can help to identify weaknesses that could be exploited by an attacker before a security incident occurs.

Figure 1-5 shows a summary and additional aspects to be addressed within the Application domain.

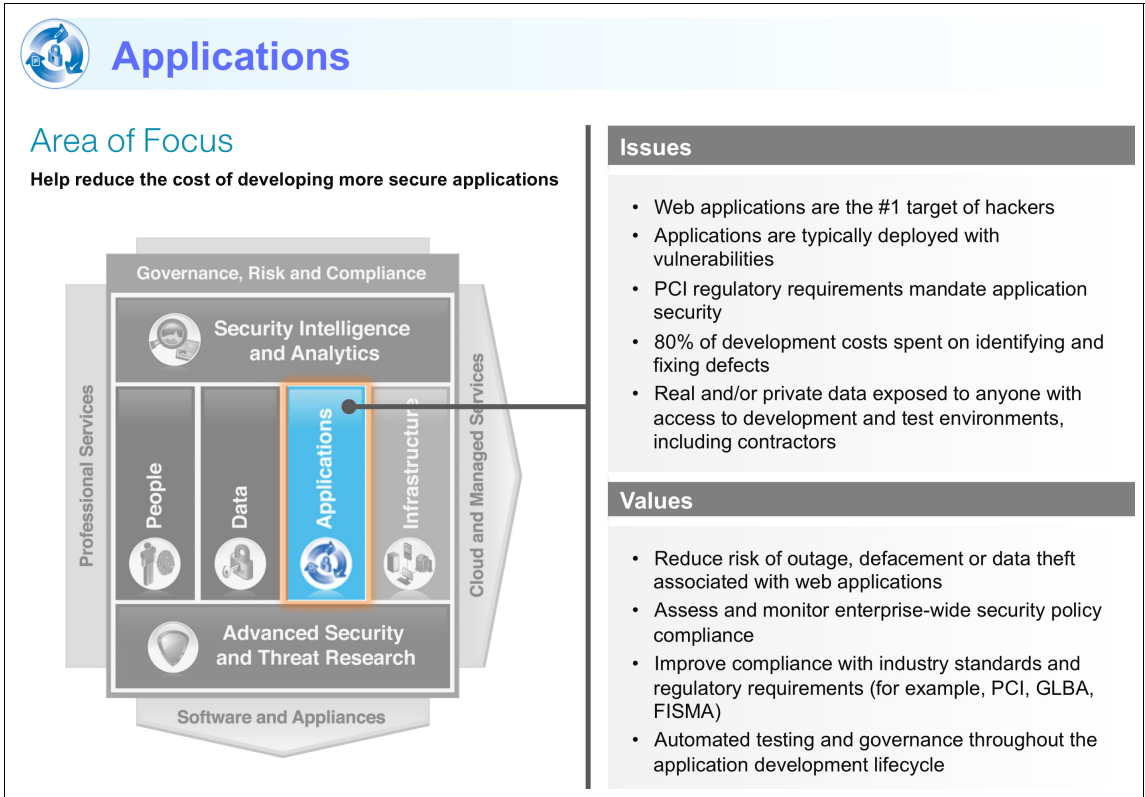


Figure 1-5 Application and Process domain

<sup>4</sup> To learn more about how IBM looks at the secure development lifecycle, download the IBM Redguide™ publication *Security in Development: The IBM Secure Engineering Framework*, REDP-4641 at <http://www.redbooks.ibm.com/abstracts/redp4641.html?Open>.



## 1.4.5 Infrastructure

Organizations must *preemptively* and *proactively monitor* the operation of the business and the IT infrastructure for *threats* and *vulnerabilities* to avoid or reduce breaches.

Security monitoring and management of an organization's network, servers, and endpoints is critical to staying ahead of emerging threats that can adversely affect system components and the people and business processes that they support. The need to identify and protect the infrastructure against emerging threats has dramatically increased with the rise in organized and financially motivated attacks. Although no technology is perfect, the focus and intensity of security, monitoring, and management can be affected by the type of network, servers, and endpoints that are deployed in the IT infrastructure and how those components are built, integrated, tested, and maintained.

Organizations are increasingly using *virtualization technology* to support their goals of delivering services in less time, with greater agility, and at lower cost. By building a structure of security controls within this environment, organizations can reap the goals of virtualization, such as improved physical resource utilization, improved hardware efficiency, and reduction of power costs, while they ensure that the virtual systems are secured with the same rigor as the physical systems.

In networks today, organizations are also faced with hundreds of new web and non-web applications that are available to their users. Social media applications, peer-to-peer file transfer applications, Voice over Internet Protocol (VoIP), web-based email, cloud data storage, and many others are all readily available. The ease and speed at which these new, and often weak, applications can be installed or simply accessed can reduce the effectiveness of a perimeter-based security architecture and provides many new types of risks. A more integrated infrastructure security solution must take these new threats into account.

Securing an organization's overall infrastructure can mean taking precautions against a failure or loss of physical infrastructure assets that might impact business continuity. This security can involve protection from indirect threats and vulnerabilities, such as the impact of the loss of a utility service, a breach in physical access control, or a loss of critical physical assets. Effective physical security requires a centralized management system that allows for correlation of inputs from various sources, including property, employees, customers, the general public, and local and regional conditions. Although securing physical infrastructure assets is as important as securing IT infrastructure assets, the remainder of this book focuses on the IT aspects of this security domain.

Figure 1-6 shows a summary and additional aspects to be addressed within the Infrastructure domain.

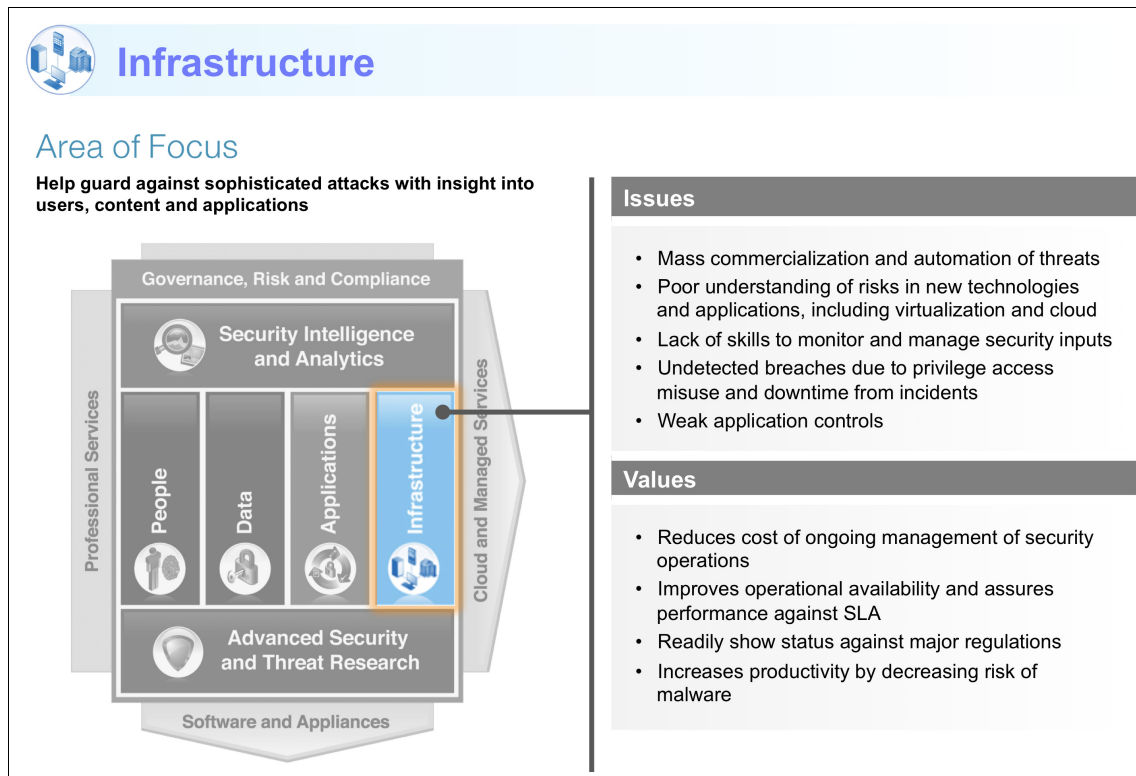


Figure 1-6 Infrastructure domain

## 1.4.6 Security Intelligence and Analytics

Security Intelligence and Analytics provides a layer of discovery and reporting on top of the security domains, that is, a control center for logging, viewing, analyzing, alerting, and reporting on events across, rather than within, domains. It provides a unified collection, aggregation, and analysis architecture for application logs, security events, vulnerability data, identity and access management data, configuration files and network flow telemetry from security applications and devices throughout the security domains. In addition, the Security Intelligence and Analytics layer provides a common platform for all searching, filtering, rule writing, and reporting functions as well as a user interface for log management, risk modeling, vulnerability prioritization, incident detection, and impact analysis tasks.

The comprehensive nature of the security intelligence architecture implies the collection of vast amounts of both real-time and historic data for alerting as well as forensic analysis. The reduction of potentially billions of items of security data into a manageable set of actionable items, and the identification of patterns of behavior that fall outside the norm, are the province of the analytics within this layer. This action requires the ability to correlate data and scale across multiple data types and sources beyond the ones that are found in the individual security domains.

Figure 1-7 shows the Security Intelligence and Analytics layer in the IBM Security Framework.

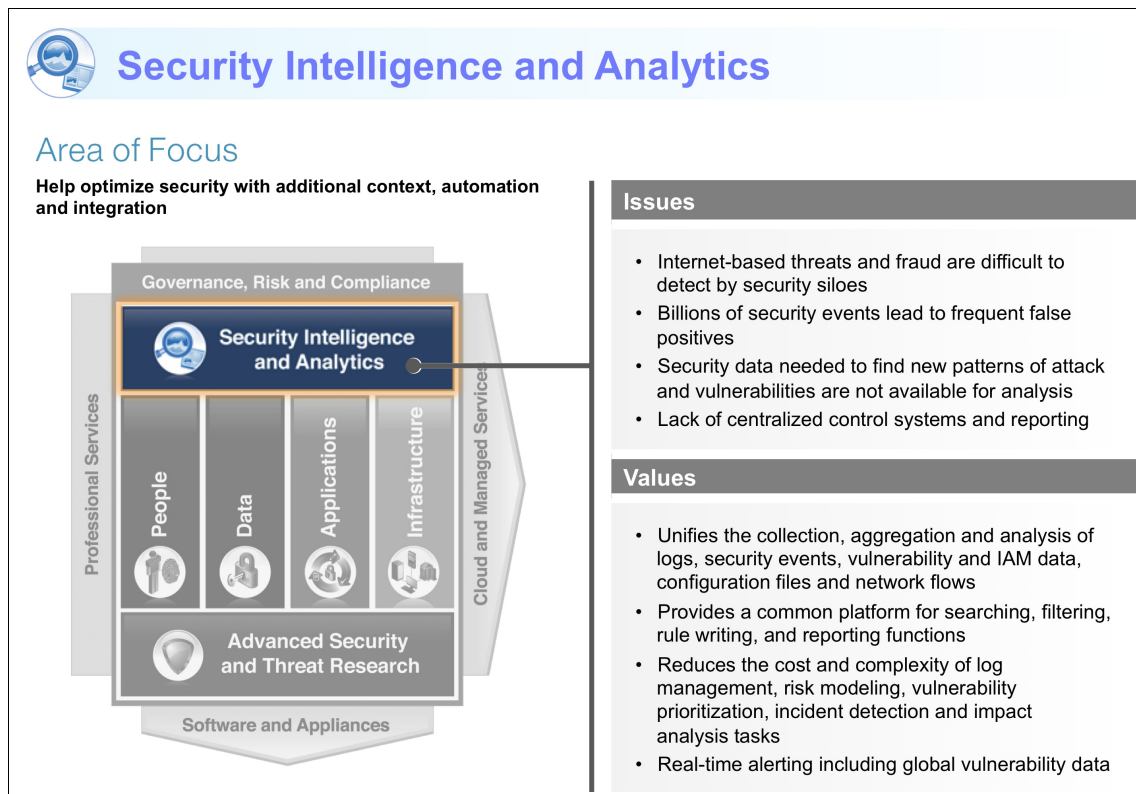


Figure 1-7 Security Intelligence and Analytics layer

### 1.4.7 Security maturity model

The IBM Security Framework provides a reference model for the security domains by which an organization can protect its people, data, applications, and infrastructure. Within each domain, there can be varying degrees of protection, from minimal, or basic, through proficient to optimized.

Organizations vary in their ability or intent to deploy security solutions depending on their budgets, experience, skill sets, and risk appetite. They might have many years of experience with user access controls, for example, with advanced, automated technology that is deployed at the optimized level in the People domain. At the same time, they might be in their first implementation of application scanning, so would be likely to be at a basic level of security in that domain.

To help clarify the security controls representative of these maturity levels within each domain, IBM developed the Security Maturity Model that is shown in Figure 1-8.

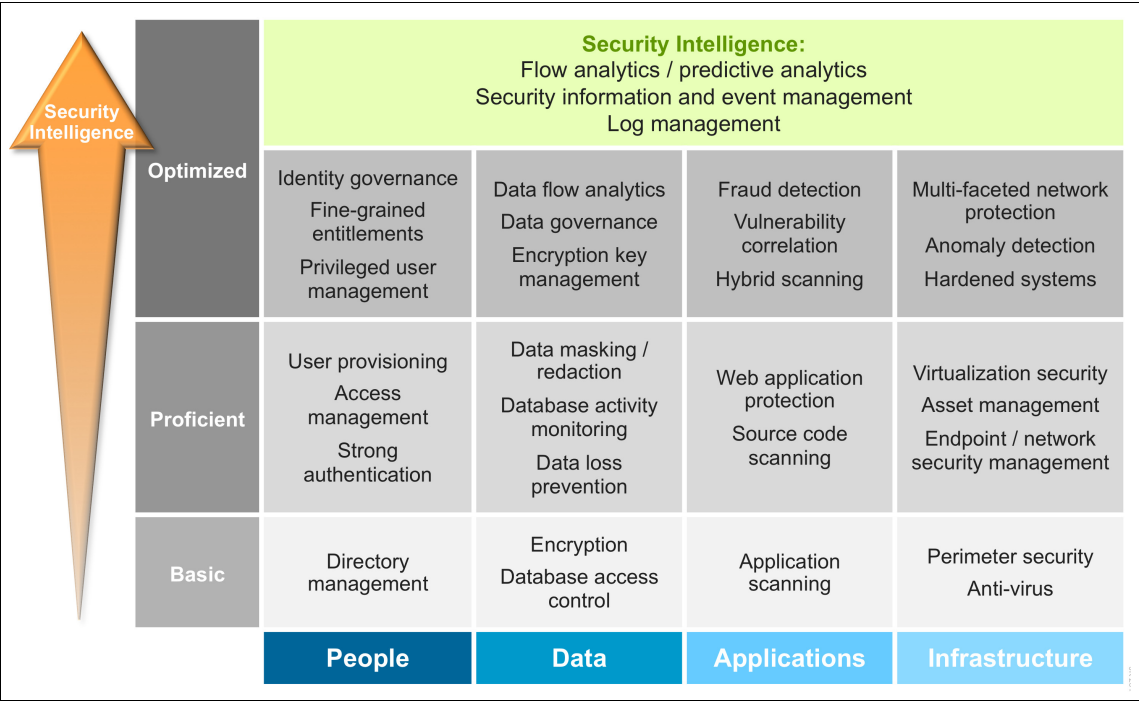


Figure 1-8 The security maturity model

Encryption and database access control are representative of a basic level of data protection, for example. To have an optimized level of data security, the organization must deploy security solutions that provide controls at the basic, proficient, and optimized level that is shown in the figure. The more optimized the security level, generally the more automated and proactive the security solution is, and the more integrated it becomes with the Security Intelligence and Analytics layer that sits above and across all of the domains.

## 1.5 IBM Security Blueprint

The IBM Security Framework divides the area of business-oriented IT security into four major security domains and three support layers. The next step is to break these domains and layers down into further detail to work toward a common set of core *security capabilities* that are needed to help an organization securely achieve its business goals. These core security capabilities are called the *IBM Security Blueprint*.

The IBM Security Blueprint uses a product- and solution-neutral approach to categorize and define security capabilities and services that are required to answer the business concerns in the IBM Security Framework.

The IBM Security Blueprint was created after research into many customer-related scenarios that were focused on how to build IT solutions. The intention of the blueprint is to support and help design and deploy security solutions in your organization.

Building a specific solution requires a specific architecture, design, and implementation. The IBM Security Blueprint can help you evaluate these items, but does not replace them. Using the IBM Security Blueprint in this way can provide a solid approach to considering the security capabilities in a particular architecture or solution.

IBM chose to use a high-level service-oriented perspective for the blueprint that is based on the IBM service-oriented architecture approach. Services use and refine other services (for example, policy and access control components affect almost every other infrastructure component).

To better position and understand the IBM Security Blueprint, see Figure 1-9.

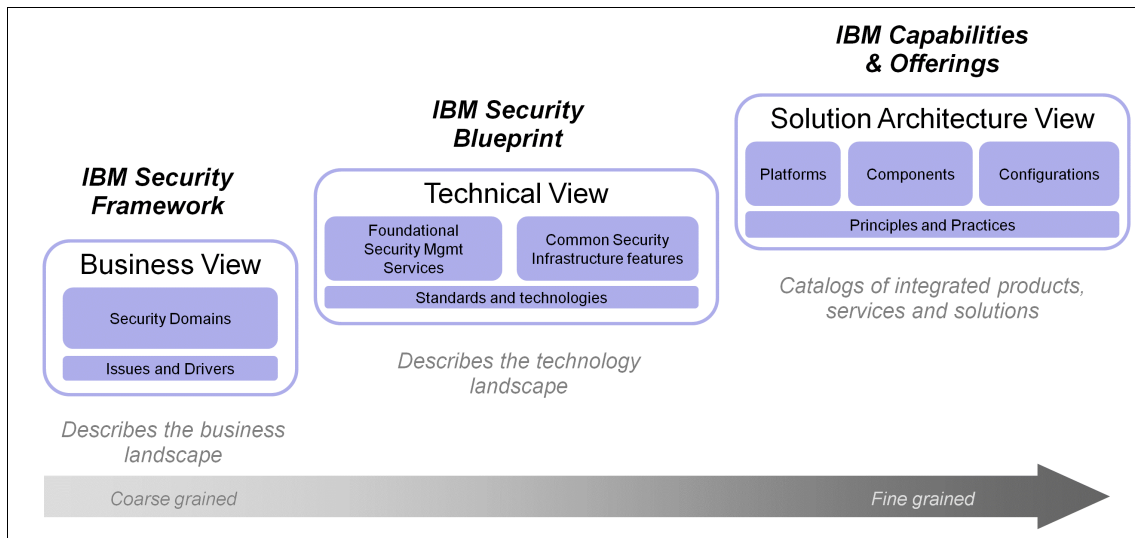


Figure 1-9 IBM Security Blueprint positioning

The left portion of Figure 1-9 represents the IBM Security Framework, which describes and defines the security domains from a business perspective. It was covered in 1.4, “IBM Security Framework” on page 8.

The middle portion in Figure 1-9 represents the IBM Security Blueprint, which describes the IT security management and IT security infrastructure capabilities that are needed in an organization. As described earlier, the IBM Security Blueprint describes these capabilities in product and vendor-neutral terms.

The right portion of Figure 1-9 represents the solution architecture views, which describe specific deployment guidance particular to an IT environment and the current maturity of the organization within the respective security domains. Solution architecture views provide details about specific products, solutions, and their interactions.

Figure 1-10<sup>5</sup> shows the complete IBM Security Blueprint, and each layer and component is described in the following sections.

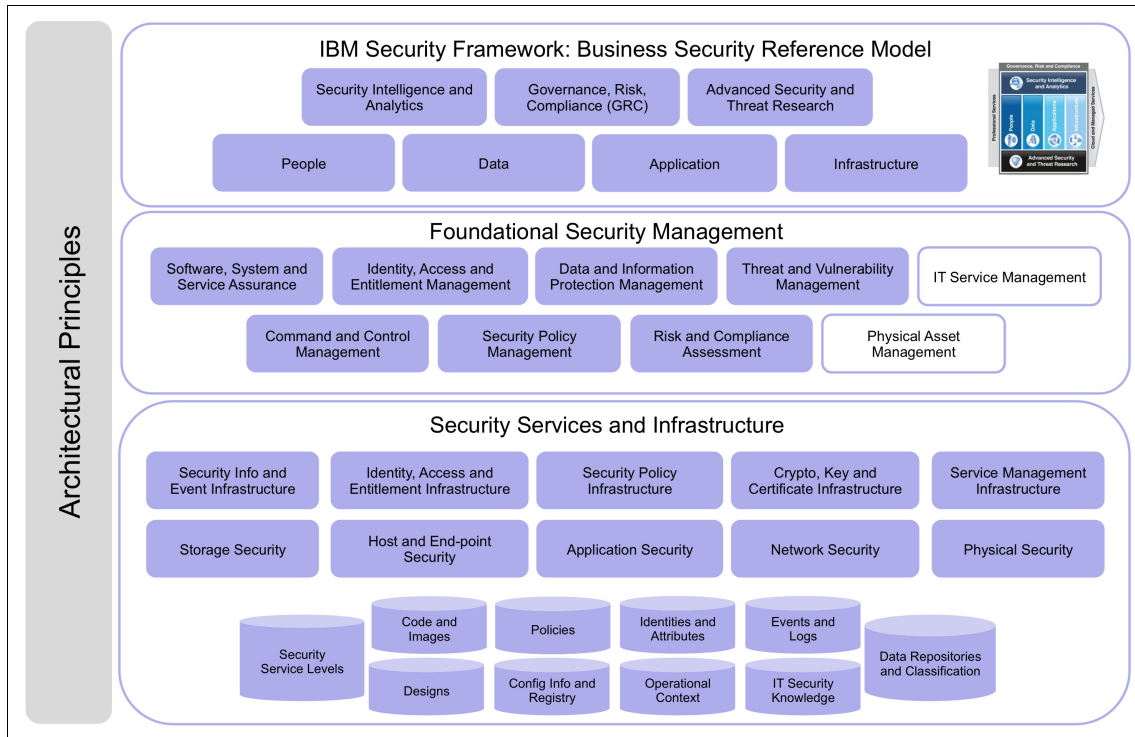


Figure 1-10 The IBM Security Blueprint

### 1.5.1 Foundational Security Management

The Foundational Security Management layer contains the top-level components that are used to direct and control IT security from a policy-based, risk management perspective. These components are described in more detail in Chapter 2, “The components of the IBM Security Blueprint” on page 31.

<sup>5</sup> White boxes in Figure 1-10 on page 23 and other diagrams represent services or components that are not solely security-related, but might be connected with other IT service areas as well.

Here is a closer look at each Foundational Security Management component:

- ▶ *Risk and Compliance Assessment* enables the IT organization to collect, analyze, and report security information and security events to identify, quantify, assess, and report on IT-related risks that can contribute to the organization's operational risk. Security dashboards provide situational awareness to allow day-to-day risk management. This component covers *risk aggregation and reporting, IT security risk processes, business controls management, resiliency and continuity management, compliance reporting, and legal discovery services*.
- ▶ *Command and Control Management* provides the command center for *security management and the operational security capabilities* for IT as well as non-IT assets and services to ensure protection, response, continuity, and recovery.

Command and Control Management fulfills both a strategic and a tactical role. The strategic role involves defining security policies. The tactical role involves coordination of the security operations. It covers topics such as:

- Ensuring that physical and operational security is maintained for locations, assets, humans, environment, and utilities
  - Providing surveillance and monitoring of locations, perimeters, and areas
  - Providing top-level incidents that are delivered by security intelligence and analytics for further investigation
  - Enforcing entry controls
  - Providing for positioning, tracking, and identification of humans and assets
  - Providing a focal point for continuity and recovery operations
- ▶ *Security Policy Management* provides all capabilities and repositories to author, discover, analyze, transform, distribute, evaluate, and enforce security policies.

Security Policy Management involves defining the security policies that are aligned with the business goals about how to reach compliance levels and mitigate risks to an acceptable level. It deals with setting up a governance framework to define and enforce policies and measure their effectiveness, reporting back to Governance, Risk, and Compliance.

- ▶ *Identity, Access, and Entitlement Management* provides capabilities that are related to roles and identities, access rights, and entitlements. The correct usage of these capabilities can ensure that access to resources is given to the correct identities, at the correct time, and for the correct purpose. These services can also ensure that access to resources is monitored and audited for unauthorized or unacceptable usage.



- ▶ *Data and Information Protection Management* provides capabilities that protect unstructured and structured data from unauthorized access and data loss, according to the nature and business value of information. It also provides usage and access monitoring and audit services.
- ▶ *Software, System, and Service Assurance* addresses how software, systems, and services are designed, developed, tested, operated, and maintained throughout the software lifecycle to create predictably secure software. This component covers the following items:
  - Structured design
  - Threat modeling
  - Software risk assessment
  - Design reviews for security
  - Source code reviews and analysis
  - Dynamic application analysis
  - Source code control and access monitoring
  - Code and package signing and verification
  - Quality assurance testing
  - Supplier and third-party code validation
- ▶ *IT Service Management* provides the process automation and work flow foundation for security management. In particular, change and release management processes play a significant role in security management.
- ▶ *Threat and Vulnerability Management* provides capabilities that identify vulnerabilities in deployed systems and receive reports of vulnerabilities from outside sources, determine the appropriate response, and make proactive changes to deployed systems to maintain the security of the deployed system. Other capabilities collect security events and information from a wide range of sources to gain insight and detect possible threats through event correlation and security intelligence and analytics.
- ▶ *Physical Asset Management* provides awareness of the location and status of physical assets as well as awareness of physical security controls and coordinates the security information for physical systems with the IT security controls.

## 1.5.2 Security Services and Infrastructure

The Security Services and Infrastructure layer contains components and subcomponents that are used by the Foundational Security Management components in their respective contexts:

- ▶ *Security Information and Event Infrastructure* provides the infrastructure to automate log aggregation, correlation, and analysis. It also enables an organization to recognize, investigate, and respond to incidents automatically, and streamline incident tracking and handling, with the goal of improving security operations and information risk management.
- ▶ *Identity, Access, and Entitlement Infrastructure* provides services to manage user provisioning, passwords, single sign-on, access control, and synchronization of user information across directories.
- ▶ *Security Policy Infrastructure* provides services to manage the development implementation of security policies in a consistent manner and automate the deployment of those policies to IT systems.
- ▶ *Cryptography, Key, and Certificate Infrastructure* provides services to perform cryptographic operations efficiently and provides operational processes and capabilities to manage cryptographic keys.
- ▶ *Network Security* consists of multi-layered network security to provide defense in-depth, deep inspection, and analysis of protocols, application level payloads, and user content to protect at all levels of the network stack. It extends to virtual networks for security in modern and heavily virtualized environments.
- ▶ *Storage Security* provides data-centric security capabilities for protecting data in use, in transit, and at rest through isolation and encryption capabilities. It also provides services to catalog and classify storage assets and associate control policies with them.
- ▶ *Host and End-point Security* provides protection for servers and user devices, such as mobile phones, desktop computers, and mobile computers using both host and network-based technologies. This protection integrates into the virtualization infrastructure to provide security for virtual environments. It includes hardware-based attestation of host operating systems (OSes) and system resources to protect against malicious attacks.
- ▶ *Application Security* provides the infrastructure for testing, monitoring, and auditing deployed applications.
- ▶ *Service Management Infrastructure* consists of the infrastructure services to handle service management processes, such as incident, problem, change, and configuration management. Process automation is generic framework-based services to automate IT actions, including security-related activities.

- ▶ *Physical Security* is an IT infrastructure service to create awareness of physical security and coordinate it with IT security. This service can include employee badges, RFID readers, surveillance systems, and associated technology or assets. Physical Security can include automation that is related to surveillance, motion detection, object and human identification and tracking, entry control, environmental system monitoring, perimeter control, and power and utility system monitoring.

### 1.5.3 Architectural principles

IBM security architects defined the following *Architectural Principles* that accompany the service decomposition. These principles can be applied to all levels of the framework, blueprint, and solution designs, and are also guidelines for IBM products and solutions.

- ▶ Openness  
Openness is of primary importance in an enterprise environment. Openness includes support for all major platforms, run times, and languages, support for major industry standards, published interfaces and algorithms, avoiding *security by obscurity*, documented trust and threat models and support for Common Criteria, and similar formal security validation programs.
- ▶ Security by default  
Security must not be an afterthought in IT solutions; security policies must be secure immediately. This situation is helped by a consistent definition and management of configurations, a consistent set of security roles and persona across products, and a consistent security management user interface.
- ▶ Design for accountability  
With many requirements in the compliance area, it is important that all security-relevant actions can be logged and audited, the audit infrastructure is scalable to handle these events, and audit information is immutable and non-reputable.
- ▶ Design for regulations  
Regulations drive many requirements in IT security projects, and regulations change over time. Handling this situation requires flexible support for the constraints that are set by government regulations and industry standards and traceability between regulations, standards, and business policies, and the security policies that are used to implement them.

- ▶ Design for privacy

In the current age of data sharing, privacy becomes increasingly important. Solutions must highlight the usage of personally identifiable information and corresponding data protection mechanisms and enable the principles of notice, choice, and access.

- ▶ Design for extensibility

Good solutions are component-based and separate the management of mechanisms from the mechanisms themselves to support various mechanisms under the same framework. Deployed systems must allow for the addition and extension of new mechanisms within the existing management framework.

- ▶ Design for sharing

Multiple solutions can share a single IT environment, such as in a shared service center. To achieve this goal, security services and management must be able to span multiple domains, each domain potentially providing its own and independently set security policy, identity, models, and so on. Architectures must explicitly document the assumptions and limitations that are made in terms of span of control.

- ▶ Design for consumability

All security services must be easily used by various audiences. These audiences include programmers who develop and integrate applications with the security services, management systems that create, update, and manage security policies and other security artifacts, and people who manage security activities, audit security activities, and request access to protected resources.

- ▶ Multiple levels of protection

*Defense in depth* is a general principle, which can be achieved by multiple levels of enforcement and detection. Resources must be designed to protect themselves as a first layer of defense. Intrusions can be contained through *isolation* and *zoning*. Multiple levels also minimize the attack surface to the outer-most accessible layer. *Least privilege* is a similar fundamental principle. Finally, the system should incorporate fail-safe principles.

- ▶ Separation of security management, enforcement, and accountability

Security management services (identity, authorization, audit, and so on) are provided through a dedicated and shared security infrastructure, enabling consistent monitoring and enforcement. The enforcement itself (through cryptography, policy enforcement, or physical isolation) is typically distributed and kept close to the resources.

- ▶ Security-critical resources and awareness of their security context  
Resources and actors are kept aware of their environment (including physical location and logical collocation) and their security status and context.
- ▶ Model-drive security  
Models are reflective of the operating environment, common models, and consistent formats for identity and trust, data, policy, applications, security information and events, and cryptographic keys. Models are consistently interpreted across the stack (for example, network identities are linked to application-level identities) and across units (for example, policies and trust are negotiated and understood within a federation). Models are consistently validated against reality (feedback from policy and model discovery).
- ▶ Consistency in approaches, mechanisms, and software components  
Two independent layers of protection for one resource might improve security. But using two different mechanisms for the same purpose for two resources increases the chances that at least one of them fails (plus, they increase management impact).  
The IBM Security Blueprint lists the preferred standards and mechanisms.

The next chapter describes the components of the IBM Security Blueprint in more detail.





# The components of the IBM Security Blueprint

This chapter explains the IBM Security Blueprint in more detail by describing the *components* and *subcomponents* of the IBM Security Blueprint.

The components in the IBM Security Blueprint describe the common security capabilities that are needed in any IT environment to manage IT security risks. Like the other elements of the IBM Security Blueprint, the components describe these security capabilities in vendor and product neutral terms, using common, accepted industry definitions.

Each component is described in terms of the services that it provides, which can be combined with other components to create solution patterns. Key work products and artifacts for each component are also described, along with relevant industry standards.

The component descriptions often, but not always, correspond to market segments and product offerings. However, in many cases, a product offering might encompass multiple components. The intent of the components is not to describe a product or service taxonomy, but to provide a product and vendor neutral way to describe IT security capabilities.

The components are organized into two layers. The *Foundational Security Management* components comprise the first layer. Each component is decomposed into a set of more detailed subcomponent descriptions. A set of key components in the *Security Services and Infrastructure* is identified on a second layer. Although this section provides many details about the first layer, the second, more supportive layer is described more briefly because many terms should be familiar to the information technology (IT) security professional.

This chapter includes the following sections:

- ▶ Foundational Security Management
- ▶ Subcomponents
- ▶ Conclusion

## 2.1 Foundational Security Management

This section explains the Foundational Security Management *components* of the IBM Blueprint and how they work together to govern the policies and deployed security capabilities in a way that supports the business objectives. Furthermore, we introduce their respective subcomponents.



The set of Foundational Security Management components forms a closed loop management system. Figure 2-1 depicts the continuous risk management cycle as it must be practiced for comprehensive security management. *Command and Control Management* sets security directives and objectives, which are used by *Security Policy Management* in combination with industry and regulatory standard inputs to produce and set the policies and standards that must be adhered to in the other functional areas of security, as they are represented on the right side of Figure 2-1.

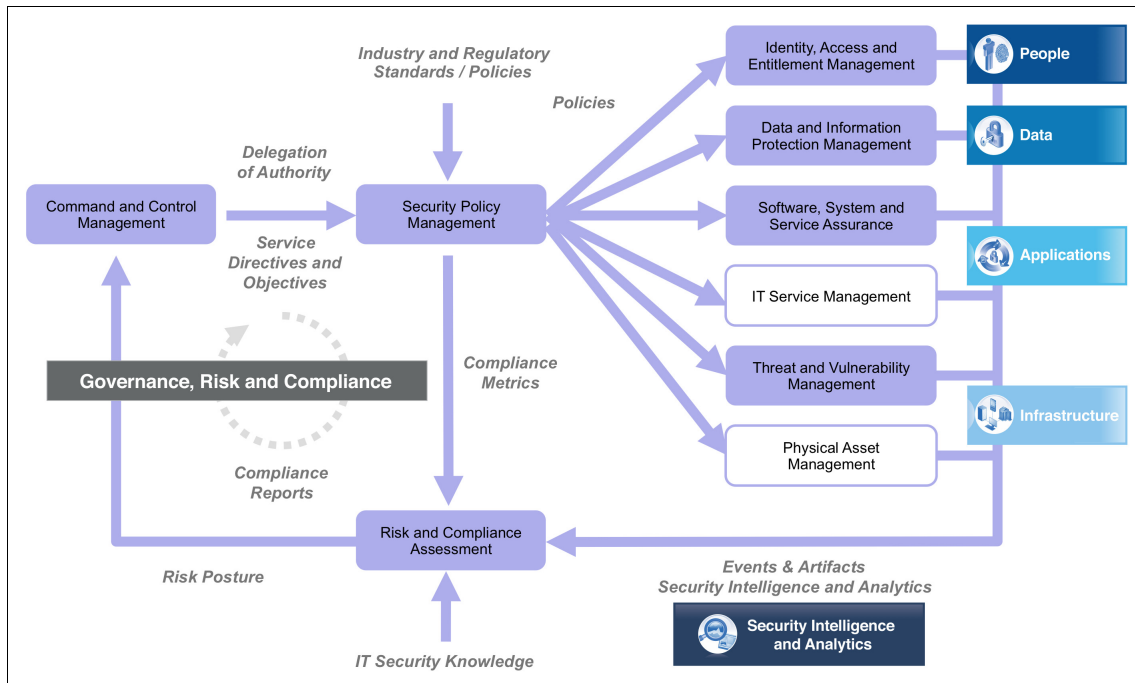


Figure 2-1 Foundational Security Management components closed loop

Also, Security Policy Management delivers the compliance metrics as input to *Risk and Compliance Assessment*, which receives the security events and artifacts that are generated by the more IT delivery-centric security components. Next, Risk and Compliance Assessment combines these events and artifacts to match them with the compliance metrics to produce compliance reports and also to derive a related risk posture, both of which can serve as input into Command and Control Management, so the information can be used for further adjustments to directives and objectives.

Figure 2-1 on page 33 also shows the security domains of the IBM Security Framework next to the respective matching Foundational Security Management services. The Command and Control Management, Security Policy Management, and Risk and Compliance Management components together reflect the Governance, Risk, and Compliance domain of the IBM Security Framework. The others have a one-to-one matching domain, except for the Application domain, which is matched by the Software, Systems, and Service Assurance component and the IT Service Management component. The Infrastructure domain also encapsulates both Threat and Vulnerability Management and Physical Asset Management components.

The next section provides further details about the Foundational Security Management components by deconstructing them into their subcomponents and listing the related common security infrastructure components.

## 2.2 Subcomponents

For each of the components on the Foundational Security Management layer, the IBM Security Blueprint provides a further deconstruction into *subcomponents*, and an alignment of key Security Services and Infrastructure components, which are essential to components in the Foundational Security Management layer. These components are presented in the following order:

- ▶ Command and Control Management
- ▶ Security Policy Management
- ▶ Risk and Compliance Assessment
- ▶ Identity, Access, and Entitlement Management
- ▶ Data and Information Protection Management
- ▶ Software, System, and Service Assurance
- ▶ Threat and Vulnerability Management
- ▶ IT Service Management
- ▶ Physical Asset Management

### 2.2.1 Command and Control Management

The Command and Control Management component provides the command center for security management and the operational security capabilities for non-IT assets and services to ensure protection, response, continuity, and recovery. It covers many topics:

- ▶ Approving authority for security.
- ▶ Ensuring that physical and operational security is maintained for locations, assets, humans, environments, and utilities.

- ▶ Providing surveillance and monitoring of locations, perimeters, and areas.
- ▶ Enforcing entry controls.
- ▶ Providing for positioning, tracking, and identification of humans and assets.
- ▶ Providing a focal point for continuity and recovery operations.

Command and Control Management encompasses situational awareness and reacting to urgent security issues. It also includes the ability to observe and react to long-term trends. In both cases, Command and Control Management includes the ability to trigger and initiate reactive and proactive changes in IT security.

Command and Control Management might use other Foundational Security Management services and can serve as the control point for them when knowledge, approval, situational analysis, risk mitigation, and delegation of authority decisions are needed. Figure 2-2<sup>1</sup> shows an overview of Command and Control Management components and the related components from the Security Services and Infrastructure layer.

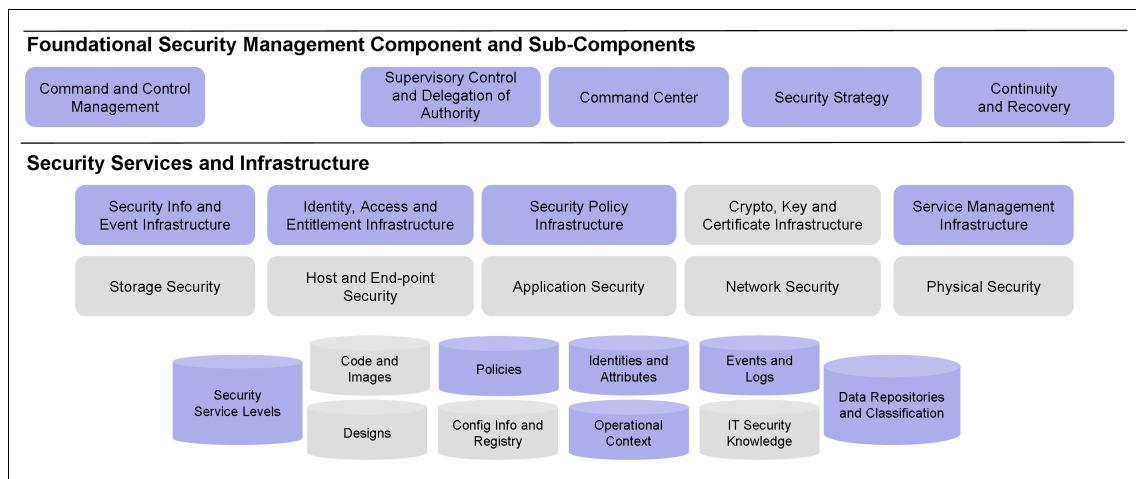


Figure 2-2 Command and Control Management subcomponents

Command and Control Management consists of the following subcomponents:

- ▶ Supervisory Control and Delegation of Authority
- ▶ Command Center
- ▶ Security Strategy
- ▶ Continuity and Recovery

<sup>1</sup> Gray boxes in Figure 2-2 and other diagrams represent services or components that might not be required for respective tasks.

These functional components are described separately to ensure that separation of duties can be achieved.

### **Supervisory Control and Delegation of Authority**

Similar to the concept of Supervisory Control and Data Acquisition<sup>2</sup> (SCADA) systems in physical plants and industrial centers, this component represents the supervisory roles in information security management. This component includes the concepts of delegating authority for IT security to the appropriate people and roles in the organization and remotely managing the IT security infrastructure.

As part of its supervisory duties, this component owns the responsibility for security as a whole and also for ensuring that policies, standards, and procedures comply with relevant elements of criminal, civil, administrative, and regulatory law to minimize adverse legal consequences.

This component is concerned with making sure that personnel and executives are safe and secure while on site or traveling for the company and knowing to whom authority should be delegated if a person becomes incapacitated or otherwise unavailable.

### **Command Center**

The Command Center represents the service organization unit that is needed to respond to immediate physical or IT security threats, either through automated responses or scripted scenarios. It also encompasses the development and deployment of crisis management procedures. The technology aspect of the command center can be an enterprise dashboard that provides a central focal point for security across a company.

The command center is also the focal point for managing communication to external organizations such as Emergency Management Services, fire, police, and other law enforcement agencies.

### **Security Strategy**

The Security Strategy is closely aligned to the overall business strategy and, hence, Command and Control Management is the lead-in for business directives and thus owns responsibility for security strategy management.

Security strategy determines the overall direction of security and security-related compliance, it determines the level of security and protection targets that must be achieved, and it sets the overall boundaries for applicable controls to be deployed to meet the targets.

---

<sup>2</sup> To learn more about SCADA, see <http://www.cpni.gov.uk/ProtectingYourAssets/scada.aspx>.

## Continuity and Recovery

Continuity and Recovery represents a service that applies a specialized set of skills, processes, and technology to recover from a major unexpected disruption or a disaster in service.

These services include emergency planning activities such as training of employees, escalation procedures, phone lists, procedures, and guidelines for all major types of emergencies, and classification of potential hazards. The services include the coordination of business continuity, that is, keeping the business running during and after a disaster with significant impact on key resources, and the coordination of disaster recovery (that is, re-establishing the key resources to a normal operations level).

## Security Services and Infrastructure components

The following Security Services and Infrastructure components are key to effective Command and Control Management (depicted as blue-shaded objects in Figure 2-2 on page 35):

- Identity, Access, and Entitlement Infrastructure

The Identity, Access, and Entitlement Infrastructure is used by all services in the Command and Control Center to delegate authority by authorizing appointed personnel to receive respective access rights.

- Security Policy Infrastructure

Security Policy Infrastructure is a key component for the Command and Control Center, as it provides access to the policy documents and also allows the *security policy owners* (the actors behind all four Command and Control Management services) to review and approve policies after they confirm that their initially intended Security Service Levels are correctly reflected in the policies. The Security Policy Infrastructure is also used by the services to provide amendment requests to the policies if required.

- Security Information and Event Infrastructure

The Security Information and Event Infrastructure enables the services of Command and Control Management to retrieve security and event information. This component can be valuable when the command center must confirm *ad hoc* occurrences of specific events during crisis management or in discussions with authorities. The Security Information and Event Infrastructure also supports Security Intelligence and Analytics layer in the IBM Security Framework.

- ▶ Service Management Infrastructure

The Service Management Infrastructure is fundamental to Command and Control Management because it relies on the Service Management Infrastructure to coordinate communication to other foundational security services. The personnel that are associated with the Command and Control Management services are also actors in the Service Management Infrastructure processes. For example, a change with an impact on security might need be approved by Supervisory Control and Delegation of Authority if the authority for approval of a specific level of changes (such as a major update to the security architecture of the network perimeter) is not correctly delegated and, hence, is above the clipping level of established delegations.

- ▶ Policies

Policies are important to the Command and Controls Management services as they, like all other foundational security services, adhere to policies irrelevant of the fact that the directions that are reflected in the policies had their origin in Command And Controls Management itself. Specific examples for policies include policies around delegation of approval authorities and related clipping levels, in addition to escalation paths.

- ▶ Security Service Levels

Security Service Levels are the key output of Command and Control Management and, hence, are the most important data item for the Foundational Security Management services.

- ▶ Identities and Attributes

Identities and Attributes holds the roles within the organization that are used in describing policies that are developed in Command and Control Management.

- ▶ Operational Context

Operational Context refers to the existing procedures and policies that are being followed in the IT organization so that Command and Control Management decisions can be made in a way that minimizes additional burden and disruption to the IT organization.

- ▶ Data Repositories and Classifications

Data Repositories and Classifications describe the information assets that are subject to the policies developed by Command and Control Management. Information assets have varying degrees of requirements for protecting confidentiality, availability, and integrity.

► Events and Logs

Events and Logs represent the evidence that is needed to assess the completeness and correctness of the security controls and to provide information that helps detect fraud and out of process changes to the environment.

2.2.2 Security Policy Management

Security Policy Management provides services and repositories to author, discover, analyze, transform, distribute, and evaluate IT security policies. This component represents a focal point for transforming the security requirements that are needed to mitigate business risks from an IT perspective.

A security policy is defined by the business and then enforced by the IT infrastructure, staff, and customers of the organization. This enforcement often results in the materialization of a security policy in technology-specific implementations, such as XACML and WS-SecurityPolicy.

Figure 2-3 shows an overview of Security Policy Management subcomponents and the related components from the Security Services and Infrastructure layer.

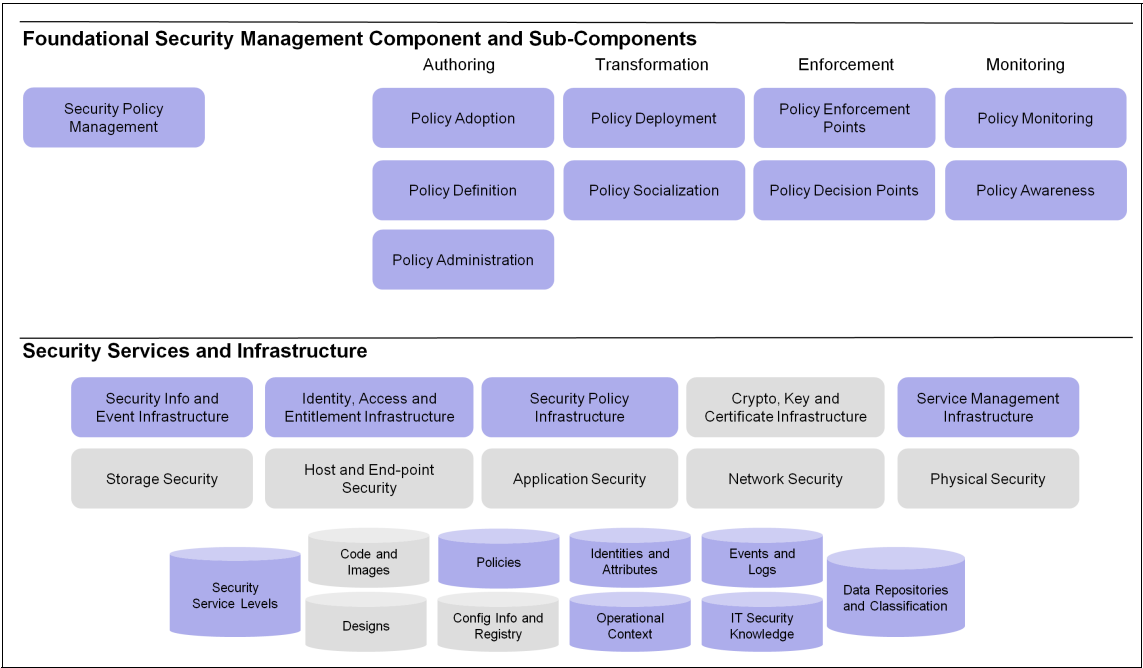


Figure 2-3 Security Policy Management subcomponents

Security Policy Management consists of the following subcomponent groups:

- ▶ Policy Authoring
- ▶ Policy Transformation
- ▶ Policy Enforcement
- ▶ Policy Monitoring

These groups are explained in more detail in the following sections.

## **Policy Authoring**

Policy Authoring covers the activities that are needed to understand policy requirements and to define and administer policies.

## ***Policy Adoption***

Policy Adoption represents the organization's capability to understand and adopt external policy requirements. This capability is a critical component towards ensuring that organizational and regulatory policy is evaluated for appropriateness and applicability for the business for which it could affect.

With growing regulatory compliance driven policies, it is important for organizations to constantly evaluate external policy changes and its adoption requirements. This approach is often important for both financial or regulatory penalty protection and industry preferred practice alignment. This subcomponent highlights gaps in the organization's policy by mapping the external policies to those policies provided from the Command and Control Management.

It is critical to note that simply complying with a regulation does not necessarily mean that security risks are mitigated as needed, or that the security control in the organization is mature enough to be effective in its implementation.

*Tick-in-the-box compliance* is not effective and does not necessarily address the organization's needs.

## ***Policy Definition***

Policy Definition is responsible for capturing the context and background of the IT security policy by tracking the upstream policy documents (internal and external) that influence it or rationalize and justify it. This subcomponent addresses policy in both non-technical and technical terms that are relevant to the organization's IT infrastructure.

## ***Policy Administration***

Policy Administration addresses the human-oriented workflow processes within the policy lifecycle management, which includes create, modify, and maintenance tasks for policies over time. It also addresses the need to manage multiple versions of a policy and transition from one to another over time.



Within the realm of Policy Administration, the policies are approved, announced, published, and commenced as part of Policy Transformation. Also, related activities for this subcomponent include policy education, socialization, and security awareness.

## **Policy Transformation**

Policy Transformation is concerned about getting an authored policy distributed into the organization's infrastructure, including both IT systems and the human participants.

### ***Policy Deployment***

As part of the policy lifecycle management, business policies are refined to service-specific policies, such as security, performance indicators and metrics, and trust policies. The resulting security policies must be translated and distributed to the technical enforcement and decision points.

For machine-readable policies, the policies are preferably defined centrally and then distributed to the enforcement points in a canonical format (for example, XACML, WS-Policy, or WS-SecurityPolicy). The binding information to enforce the policies is also distributed appropriately. These policies are often transformed at the enforcement point to a local representation so that they can be enforced.

### ***Policy Socialization***

Not all security policy transforms into machine readable or strictly enforceable policy. It is therefore important to identify the human behavior and cultural security policies that the organization requires to mitigate risk. In an environment where policies and regulations change often, it is important to ensure alignment of business appropriate security cultures, beliefs, values, and behaviors with this change.

The dissemination of policy knowledge covers the critical gap between machine enforceable policy and humans. Without appropriate socialization, organizational security guidelines can be established outside security policy norms. As humans often refer to others for decisions before they consult documentation, Policy Socialization creates a security awareness culture based the organizational policy.

## **Policy Enforcement**

After the policies are correctly authored and transformed in the organization, they are used by IT systems to make decisions and enforce policy appropriately.

### ***Policy Decision Points***

Policy Decision Points (PDPs) represent the capability to evaluate a request and decide about whether the request is policy conformant. In certain cases, all the information that is needed to make the decision is contained within the request itself. In other cases, external context information is needed. Sometimes, the sources of context information are called Policy Information Points (PIPs).

There are important issues that affect the placement of PDPs in an IT environment. Centralization of PDPs can reduce administrative burdens and potential errors during deployment. Centralization of PDPs can also enable a PDP to serve multiple enforcement points. However, PDPs are often tightly bound to the Policy Enforcement Points for performance reasons.

### ***Policy Enforcement Points***

Policy Enforcement Points (PEPs) act based on whether the request conforms to policy. The action might be an enforcement action that permits or denies the request. The PEP might also monitor, log, and raise alerts without affecting the request.

### ***Policy Monitoring***

Finally, Policy Monitoring records events and decisions.

### ***Policy Monitoring***

Policy influences can come from both internal and external sources. These directives and objectives should be constantly monitored and fed into the policy lifecycle. Policy Monitoring also provides the internal feedback loop that causes review and revalidation of a policy based on its effectiveness in the implementation and success or failure of adherence to policy Key Performance Indicators (KPIs). Policy adherence must be measurable and that metrics can be provided to *Risk and Compliance Assessment* for continuous evaluation.

### ***Policy Awareness***

Policy Awareness can provide an effective measurement of success for the transformation and socialization activities. Policy Awareness is a critical step in establishing appropriate social and behavioral norms in an organization.

Through monitoring awareness of organizational security policies, organizations are able to ensure that valid sources of security policy are established, and that changes to policy are effectively communicated. Acknowledged awareness and revalidation of awareness can help protect the organization from policy violations

## Security Services and Infrastructure components

The following Security Services and Infrastructure components are key to effective Security Policy Management (depicted as blue-shaded objects in Figure 2-3 on page 39):

- ▶ Security Information and Event Infrastructure

The Security Information and Event Infrastructure enables the services of Security and Policy Management to be measured and KPI monitored. This component can be valuable when the organization must provide evidence of compliance with policy. This component can also help measure occurrences or violations of specific policies that might indicate a need to improve awareness or to modify a policy.

- ▶ Security Policy Infrastructure

The Security Policy Infrastructure is one of the key components for Security Policy Management, as it provides the containers for the various policies, related standards, procedures, and guidelines. It can automate the workflow for the various administration activities and the deployment and the communication with Policy Decision Points and Policy Enforcement Points.

- ▶ Service Management Infrastructure

The Service Management Infrastructure provides the communication and coordination channels for Security Policy Management to reach all delivery units, which might not belong to security management, but perform some security delivery function and, hence, must adhere to security policies. Also, this infrastructure component provides the capability to deploy and implement policy updates in line with standardized change and release structures.

- ▶ Security Service Levels

Security Service Levels represent the key input source for Security Policy Management, as they set the overall targets that must be decomposed in more detail and then reflected in policy directions and related standards.

- ▶ Policies

Policies represent the key output of Security Policy Management and the most frequented data item for Policy Administration, Policy Decision Points, and Policy Enforcement Points.

► Operational Context

Operational Context is important for the policy definition service in Security Policy Management. The policies that are set for an environment should be achievable to a large extent, so it is important to establish the targeted controls that are documented in the policies with consideration of their achievability and their appropriateness. The Operational Context provides essential input for related evaluations of controls. This component also helps you to avoid the situation in which a policy must be accompanied with many policy exceptions to stay in control of the deviations of the deployed operational environment from the intended (and practically unachievable) state that is set out in the policies. An unnecessary number of exceptions also requires avoidable administrative effort and leads to inefficient Security Policy Management, so evaluating the Operational Context thoroughly during the design of the policies helps to establish adequate policies and avoid situation in which policies take the form of a pure theoretical documentation.

The Operational Context is also important in Policy Administration and in Policy Deployment. Even when care is taken to establish appropriate, practical, and achievable control requirements in the policies, exceptions in an operational environment are unavoidable. Such exceptions can derive, for example, from the lack of support of a certain control by a particular system. Although compliance can be achieved in such a case, an exception is documented to capture the particular deviation from the policy and the refined requirement of compensating controls for the particular deviation. To perform these actions, the Operational Context must be examined.

► Data Repositories and Classifications

Equally important as the Operational Context, Security Policy Management services depend on reviewing and understanding the Data Repositories and Classifications. The Policy Definition service requires the structuring of the data repositories and identifying the confidentiality, integrity, and availability requirements of data repositories. Based on this information, a sufficient yet manageable set of classifications of information assets must be defined, and for each of the classifications, the related security control requirements must be set in the designed policies. As explained in the Operational Context bullet, the Data Repositories and Classifications are also examined as part of Policy Administration for the evaluation of exceptions from policy-mandated controls that are usually required for a data repository in cases in which such controls cannot be maintained for technical or business reasons.

► Identities and Attributes

Besides the Operational Context, and Data Repositories and Classifications, Identities and Attributes represent another data item that must be fully understood to define appropriate policies for an environment. Although the Operational Context helps you to evaluate the environment from a business and technical infrastructure perspective, and Data Repositories and Classifications helps you to understand it from a data and information perspective, Identities and Attributes provides the perspective onto an environment with a focus on users, administrators, and other action-takers in the environment.

As with the two aforementioned components, Identities and Attributes are taken as input to the activities of security control design in the Policy Definition service and also are used to set security requirements for these identities and the related attributes. Also, the ongoing Policy Administration service uses Identities and Attributes and its evolution throughout operations to adapt policies with new or amended requirements to address identified operational security issues and to perform continued security improvement.

► Events and Logs

Events and Logs are important because they allow verification of the completion of Security Policy Management activities, which are performed with the help of the Security Policy Infrastructure. From this perspective, the Events and Logs serve as evidential records about activities (for example, whether a specific control received review and approval from stakeholders as part of Policy Administration activities before it is published in an updated security policy). But from the perspective of Policy Definition, Events and Logs can be a helpful source of information. Along with the traditional qualitative analysis of Operational Context, Data Repositories and Classifications, and Identities and Attributes when you define appropriate controls in the security policies, event and log data from the environment can be used to identify actions and behavior that happen in that environment. This situation allows for prioritization, especially in cases in which an environment is already in operation, but to a certain extent the security policy definition lags behind. When you follow security management approaches by the book, such situations should not exist (that is, no environment should go into operation without first defining adequate security policies, but in reality this situation is not always the case). Deriving the actions that caused specific events and log records (or combinations thereof) and examining the security requirements for these actions can be helpful, especially in situations in which information about the environment is not available or fully understood, deriving security-critical actions from Events and Logs help to find a start to fix situations in which an environment lacks security policies.

► IT Security Knowledge

IT Security Knowledge for Security Policy Management services includes general knowledge about how to create and maintain effective security policies, and also requires technical understanding of the security controls provided for various platforms, in case specific security standards for these technical platforms must be established to provide clearer direction towards the implementation of respective policies. Also, general knowledge about well-established industry regulations and standards and about data privacy regulations in the various legal contexts in which an organization operates is required to better translate related directives and objectives that are coming from the business through Command and Control Management into the respective policies.

### **2.2.3 Risk and Compliance Assessment**

Risk and Compliance Assessment enables an IT organization to collect, analyze, and report security information and security events to identify, quantify, assess, and report on IT-related risks that might contribute to an organization's operational risk. This component covers Compliance Management, risk management, evidence management, and supervisory services.

Figure 2-4 shows an overview of the Risk and Compliance Assessment subcomponents and the related components from the Security Services and Infrastructure layer.

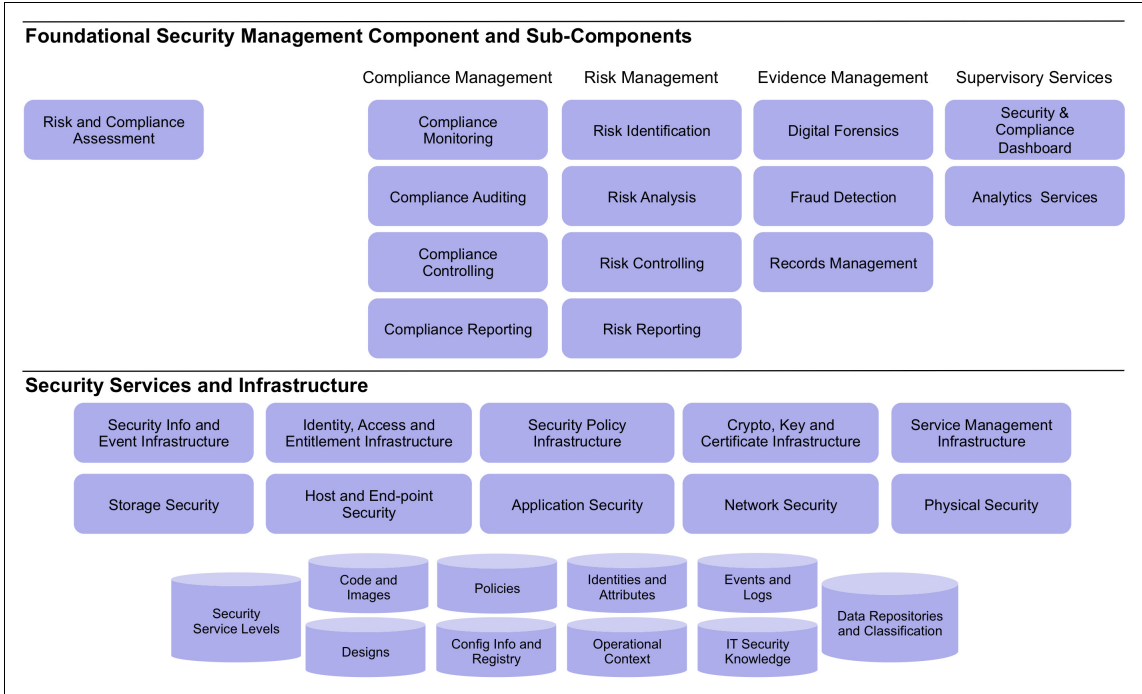


Figure 2-4 Risk and Compliance Assessment subcomponents

Risk and Compliance Assessment consists of the following subcomponent groups:

- Compliance Management
- Risk Management
- Evidence Management
- Supervisory Services

These four groups are described in more detail in the following sections.

### Compliance Management

Compliance Management covers all activities that are related to overlooking and driving the security compliance state of the IT environment.

### ***Compliance Monitoring***

Compliance Monitoring refers to the observation of the environment to identify gaps between the actual operations, the internal policies and standards, and the requirements as they derive from external industry regulations, laws, and orders.

### ***Compliance Auditing***

Compliance Auditing refers to the ability to match event sources and their event streams to compliance reporting requirements for IT security and produce reports that are based on those event streams, either periodically or on demand as part of an audit. Managing the association between the event sources reports and the compliance reporting requirement is a key capability of this component. Also, compliance requirements often impose record retention requirements on audit data, which might be different from the retention requirements for the event streams in the IT environment in general. From an IT operations perspective, the event streams are more short lived, while data that supports compliance audits might have a life span of multiple years.

### ***Compliance Controlling***

Compliance Controlling stands for the continuous work that is contributed by IT security compliance experts throughout the various parts of an organization, focusing mostly on two key activities:

- ▶ Compliance support
- ▶ Compliance tracking

*Compliance support* refers to providing advice and guidance to users who are not necessarily compliance experts, but whose activities are subject to compliance. For example, compliance experts work with a business unit to help them prepare for an upcoming audit or to help during an audit. Similar to an attorney of law in court, a compliance expert can help an audited business unit with the preparation of paperwork that is requested by the auditors or in the preparation of audit interview partners for their meeting with the auditors.

The other aspect of Compliance Controlling is *compliance tracking*, which covers the structured documentation of follow-up activities after an audit and the progress of these activities until closure. The activities are either determined by the auditor directly or are derived by an analysis of audit results as those actions, which must be implemented to mitigate identified compliance and security issues.

Compliance Controlling is a continuous process (*before, during, and after the audit*) and, hence, requires substantial ongoing efforts of a well-functioning compliance regime in an organization.



### ***Compliance Reporting***

Compliance Reporting refers to the ability to summarize analyzed event data and other security-relevant information for the specific use of demonstrating compliance. Most often, reporting is used to assess regulatory compliance or compliance with security service level agreements and overall compliance performance of the IT environment. From an internal security perspective, Compliance Reporting is most commonly used to demonstrate control over security policies and to identify trends in security compliance.

### **Risk Management**

Risk Management covers all the activities that are related to overlooking and driving the security risk posture of the IT environment.

#### ***Risk Identification***

Risk Identification refers to the ability to discover, recognize, and verify the existence of specific risks. It also encompasses the structuring of risk by mapping it into clearly defined classification schemes that can be specific to the industry or even to the risk taxonomy of an individual organization.

#### ***Risk Analysis***

Risk Analysis refers to activities that are related to the categorization, qualification, or quantification of the likelihood and impact of risks. It also covers the investigation of connections, dependencies, and correlations among various risks.

#### ***Risk Controlling***

Risk Controlling covers the determination of activities that can be used to address risks. The valid activities can range from *risk acceptance* over different approaches of *risk mitigation* to *risk transfer*. Risk Controlling also includes the determination of costs for such activities and the identification of potential risk and risk mitigation owners and actors. Another important part of Risk Controlling is tracking the status of identified and agreed risk mitigation activities until their closure.

#### ***Risk Reporting***

Similar to Compliance Reporting, Risk Reporting refers to the ability to summarize analyzed risk data and other risk-relevant information and to provide different levels of detail about the security risk posture to different parts of the organization as input for further analysis and processing.

To a certain degree, Risk Reporting is also used as input into Compliance Reporting because certain regulations might require that an organization provides information about key risk events to its stakeholders (for example, banks must inform regulatory authorities about their operational risk, which also includes their security risk posture). From an internal security perspective, Risk Reporting is most commonly used to help make the correct decisions for investments in risk mitigation activities and to track the progress for these activities.

## **Evidence Management**

Evidence Management covers services that are related to capturing and securing information in a form that can be used as legal evidence in court or that must be preserved for other legal reasons.

### ***Digital Forensics***

Digital Forensics refers to the ability to retrieve and preserve the state of IT components that are subject to a legal investigation. In certain cases, forensics simply involve preserving the state of a system for future reference. In other cases, forensics require the recreation of events that lead to the state of a particular component. For example, email is often subject to e-discovery requests in legal proceedings, and many organizations must be able to enforce *deletion holds* on email to prevent their destruction when subject to discovery proceedings.

As another example, a timeline of configuration changes for a database might need to be re-created to identify why it failed and who authorized the changes that caused the failure.

Forensics investigations can be initiated internally or as part of a legal proceeding. When forensics investigations are initiated as part of legal proceedings, more security issues can come into play, such as completeness and accuracy of the collected data, and chain of custody issues. The chain of custody issues cover situations in which data is transferred from one IT component to another or from one individual to another.

### ***Fraud Detection***

Fraud Detection covers the analysis of information and events within the IT environment that is related to unsolicited business-level activity. Usually, Fraud Detection addresses the review of security information and events for a specific combination of occurrences, which not only indicate the abuse of user rights or bypassing of access controls in a pure policy context, but are targeted to perform fraudulent activities in a criminal and legal context.

### ***Records Management***

Records Management refers to the industry term that addresses the legal requirement to capture and keep specific records about business transactions and communications for potential submission as incriminating or discharging evidence.

### ***Supervisory Services***

Supervisory Services in Risk and Compliance Management provide monitoring, alerting, and analysis across all areas of compliance, risk, and evidence management.

### ***Security and Compliance Dashboard***

Like other business-related dashboards, the Security and Compliance Dashboard refers to a set of web interfaces to display the most current relevant reporting information for IT security events and the status and completeness of compliance efforts. Dashboards are based on event streams that are collected over a period.

### ***Analytics Services***

Analytics Services helps you to find trends in correlated events and to make decisions that are based on the trends found. For example, an event analytics engine might match authorization events against human resources employee records to detect the usage of orphaned accounts for people who left the company, possibly indicating an attack from an ex-employee, or the use of a shared ID that is disallowed by corporate security policy.

In another example, a business activity monitoring control might require that each invoice be paired with an authorized purchase order. There might be multiple channels for purchase orders to come into the order system, each with a business event monitor sending purchase order event to the event correlator. Likewise, there might be two channels for invoices to be entered into the order system, each monitored by a business control that sends invoice events to the correlator. The event correlator might group these events into pairs that are based on the purchase order number, but emit a higher level invalid invoice event if it holds an invoice for more than 24 hours without receiving a corresponding purchase order event. The analytics engine can look for common patterns in the invalid invoice events and raise alerts to the appropriate departments or business control personnel.

## Security Services and Infrastructure components

The following Security Services and Infrastructure components are key for an effective Risk and Compliance Assessment (depicted as blue-shaded objects in Figure 2-4 on page 47):

- Security Information and Event Infrastructure

The Security Information and Event Infrastructure is an important element for Risk and Compliance Assessment because it can help collect and provide information about events in a synthesized, consolidated, platform-independent, and less technical format. The aggregation of security logs and subsequent derivation of security information, which now is understandable by less technical people on the business level, is provided to the Risk and Compliance Assessment services to further analyze data in a risk context (that is, in terms of probability and business impact). In the context of Compliance Management, the Security Information and Event Infrastructure can help produce reports that are designed for compliance to particular regulation and legal requirements. This infrastructure component also provides a substantial part of the evidence that must be gathered and analyzed by the Evidence Management services.

Besides providing services *for* Risk and Compliance Assessment, the Security Information and Event Infrastructure itself is also *subject to* Risk and Compliance Assessment.

- Identity, Access, and Entitlement Infrastructure

The Identity, Access, and Entitlement infrastructure is used by the Risk and Compliance Assessment services to analyze risk and compliance posture that pertains to insufficient separation of duty. Also, this infrastructure is used by the Risk and Compliance Assessment services to identify, verify, and further investigate activities of events that result from malicious user behavior.

Besides providing services *for* Risk and Compliance Assessment, the Identity, Access, and Entitlement Infrastructure itself is also *subject to* Risk and Compliance Assessment.

► Security Policy Infrastructure

The Security Policy Infrastructure provides structured access to the security policies and standards of an IT organization. Ideally, this infrastructure serves as the sole instance for compliance requirements and, thus, provides compliance-related information in an *end-to-end* fashion. End-to-end in this context implicates that the Security Policy Infrastructure must cover all possible applications and platforms and provide correct cross-referencing between the various compliance-related documents and, ideally, the individual requirements in these documents. The Security Policy Infrastructure should follow the usual pyramid structure of a compliance documentation framework, with the top-level security policy and more detailed security policies and corresponding technical security standards underneath.

As policies and standards develop and change over time, the Security Policy Infrastructure is not only able to provide a snapshot of the policy framework at a certain point in time, but it supports the evolution of policies and standards. It allows the recording of the state of approval for a policy at a certain point in time and provides convenient ways to examine differences between various compliance requirements. This situation can help identify and resolve potential contradictions between policies to prevent misunderstandings about the direction or the intent of a compliance requirement.

Finally, the Security Policy Infrastructure helps you to check whether the policy workflow for defining and establishing security policies and standards were correctly followed. From this perspective, the Security Policy Infrastructure itself must comply with requirements of the policies and standards that it holds and, thus, it is also subject to audits and reviews.

A policy infrastructure that is defined in this way can serve as a single consolidated reference of the intended state of compliance for any organization. It can be the key to an efficient security and Compliance Management implementation.

► Cryptography, Key, and Certificate Infrastructure

The Cryptography, Key, and Certificate Infrastructure provides the capability to perform cryptographic operations. As such, it is not directly used by the Risk and Compliance Assessment services. However, many organizations that use the Cryptography, Key, and Certificate Infrastructure must abide by rigid laws and regulations on encryption key lengths and methods. That is why the Cryptography, Key, and Certificate Infrastructure is an area that must be thoroughly assessed by Compliance Management.

- ▶ Service Management Infrastructure

Risk and Compliance Assessment services operate under an agreed-upon Service Management Infrastructure and must use the services that are provided by that infrastructure. For example, accessing and transferring evidence from audited machines must be performed in line with the change management process (for example, they must use correct Change Management ticketing and approval, and thus use the Service Management Infrastructure). Equally important, Evidence Management activities must be performed in line with incident and problem management processes and use the related parts of the Service Management Infrastructure (for example, mechanisms that are provided for incident and problem logs).

- ▶ Storage Security

Storage Security is tied to Risk and Compliance Assessment both from a direct and from an indirect perspective.

From a direct perspective, Storage Security is a target of many Risk and Compliance Assessment services, which means that Storage Security is assessed and examined by these services.

From an indirect perspective, Storage Security is heavily used by all five management infrastructures (that is, Security Policy Management Infrastructure, Event and Log Management Infrastructure, Cryptographic Key Management Infrastructure, Identity and Access Management Infrastructure, and Service Management Infrastructure) required by the Risk and Compliance Assessment services. Risk Management, Compliance Management, and Evidence Management have high requirements for the integrity on stored data.

- ▶ Host and Endpoint Security

Host and Endpoint Security provides an indirect service to the Risk and Compliance Assessment component through the five security management infrastructures because all the infrastructure components run on actual hosts and use endpoints. Host and Endpoint Security is important for these management infrastructures to function. Several of those important services include agents and collectors that must be distributed to the hosts and endpoints for the security management and aggregation layer infrastructure to be able to serve their purpose.

From a direct perspective, Host and Endpoint Security is a key examination point for Risk, Compliance, and Evidence Management services. Besides managing security aspects for physical systems, Host and Endpoint Security includes security configuration details for operating systems, middleware, software packages that provide a distinct security function, like antivirus software, personal firewalls, host intrusion detection and prevention systems, and hard disk, file, or mail encryption software.

- ▶ Application Security

Application Security provides many events and logs that must be analyzed for risk and compliance. Because it is the closest and most used interface for the business user, it is important that it is examined for Compliance Management and Evidence Management, especially for fraudulent activities.

- ▶ Network Security

Like many of the other technical platforms, network components and traffic provide a wide range of traces of events and general activities, which are considered important factors for all Risk and Compliance Assessment services.

- ▶ Physical Security

Physical Security, like the security of any of the technical platforms, can consist of a wide range of security controls that must be functional to fulfill compliance requirements to mitigate risks and retain evidence.

Physical Security is essential because information that must be protected does not exist only in electronic forms, but also in traditional non-electronic forms. Good security practices require the management of the risks, compliance, and related evidence in the physical domain as well.

- ▶ Security Service Levels

Because the Security Service Levels provide the background for the policies, Risk and Compliance Assessment services can use them to understand and resolve potential different interpretations and ambiguities in the security controls and the security control objectives that are defined in the policies and, hence, in the measurement of compliance.

Also, Security Service Levels can be examined by Risk and Compliance Assessment services to evaluate whether they can cause risks by themselves and must be adjusted.

- ▶ Code and Images

Code and Images are used to identify potential sources of risk and of non-compliance. Those risk and non-compliance issues might surface only on systems that are in production, but the issues have their origin in flaws in the source code and the base images. Comprehensive security policies typically define requirements and controls onto the source code and image composition themselves so that Risk and Compliance Assessment services must assess them before they are being put into production.

► Designs

Designs are important to Risk and Compliance Assessment services because they are used as (often graphical) representation systems, users, and processes and their relationships. Such representation must reflect the respective security policies, standards, and directives. Risk and Compliance Assessment services assess the designs and architectures for risks and for compliance within policy and regulatory requirements and also use them as reference for an intended state of something that is implemented. In other words, Risk and Compliance Assessment services must verify whether the designs are in line with security and compliance requirements, and then again whether the implemented environment is in line with this verified design.

► Policies

One of the primary inputs into Risk and Compliance Assessment are the Policies. They define the compliance metrics that are used to identify non-compliance for many systems and services. Compliance Management assesses compliance of the IT environment by identifying and examining differences between actual and intended compliance values that are defined in the compliance metrics. Risk Management assesses the compliance metrics and the target values for the adequacy for mitigating related risks to the level set by Command and Control Management as acceptable.

► Configuration Information and Registry

The Configuration Information and Registry contains settings that must be implemented to meet security controls that are defined in the policies. Compliance Management uses this information to verify that the security controls are correctly implemented and, thus, compliance requirements are met. Risk Management assesses the configuration for the technical appropriateness of the settings to verify that risk mitigation targets are met. Evidence Management assesses the Configuration Information and Registry for any suspicious unauthorized changes that might allow fraudulent activities. Evidence Management also collects evidence about the security state of the IT environment when it is required from a legal perspective.



► Identities and Attributes

Directories contain important information about people's identities along with other key attributes, which is used to control access to data and other resources. Hence, major efforts within the Risk and Compliance Assessment services are focused on checking the compliance posture and the risks that derive from errors in Identities and Attributes. Although the Identity, Access, and Entitlement Management infrastructure is assessed from the perspective of procedural compliance, the Identities and Attributes are assessed from a perspective of factual or conclusive compliance. Both in combination can also reveal whether the Identity, Access, and Entitlement Management services function as designed or whether they were bypassed to make changes in Identities and Attributes. The Evidence Management services require access to Identities and Attributes to gather evidence about identities that were used to perform potentially malicious behavior.

Besides assessing the technical compliance and related risks in the area of identity and access management, Risk and Compliance Assessment services assess identity and attributes information also from a more organizational perspective. The risk and compliance experts must not only check and verify whether technical settings for access administration are correct, but also whether the entitlements of a certain user for a certain resource are appropriate from a compliance and risk perspective. For example, information access should not be granted to a user with specific *identity features*, such as nationality, security clearance, or location of that user. In another example, the information might be classified so that it cannot be changed by one user alone, who must have another user help him (the four-eye-principle).

► Operational Context

The Operational Context can influence whether an activity and, hence, related events are compliant or non-compliant. That is why the Operational Context must be reviewed by Risk and Compliance Assessment services to come to the correct conclusions about compliance and evidential material and about risk.

An example of such influence can be the execution of privileged activities with an unrestricted account. Although an administrator might be granted, from a technical perspective, unrestricted access to a system, this administrator should use only a limited subset of commands to perform a change. Hence, the execution of other privileged commands that are not related to this particular change, although still being perfectly OK for a different task, could be discovered by checking the Operational Context.

- ▶ IT Security Knowledge

Defining the appropriate risk categories and applying security risk thinking requires specific experience and IT Security Knowledge. IT Security Knowledge for Risk and Compliance Assessment also includes detailed understanding of compliance and regulatory standards.

- ▶ Data Repositories and Classification

Data repositories are increasingly incorporating access control mechanisms to create an access control point as close to the data as possible. The classifications of the data in repositories must be compliant and set in a way that can possibly reduce risk to an acceptable level. Also, as evidential data must be stored in data repositories (even if the repositories are taken offline), the access and the classification of this data is paramount to keeping them admissible for any legal activities.

## **2.2.4 Identity, Access, and Entitlement Management**

Identity, Access, and Entitlement Management provides services that are related to roles and identities, access rights, and entitlements. The correct usage of these services can ensure that access to resources is granted to the correct identities, at the correct time, and for the correct purpose. These services can also ensure that access to resources is monitored and audited for unauthorized or unacceptable usages.

Figure 2-5 shows an overview of Identity, Access, and Entitlement Management subcomponents and the related components from the Security Services and Infrastructure layer.

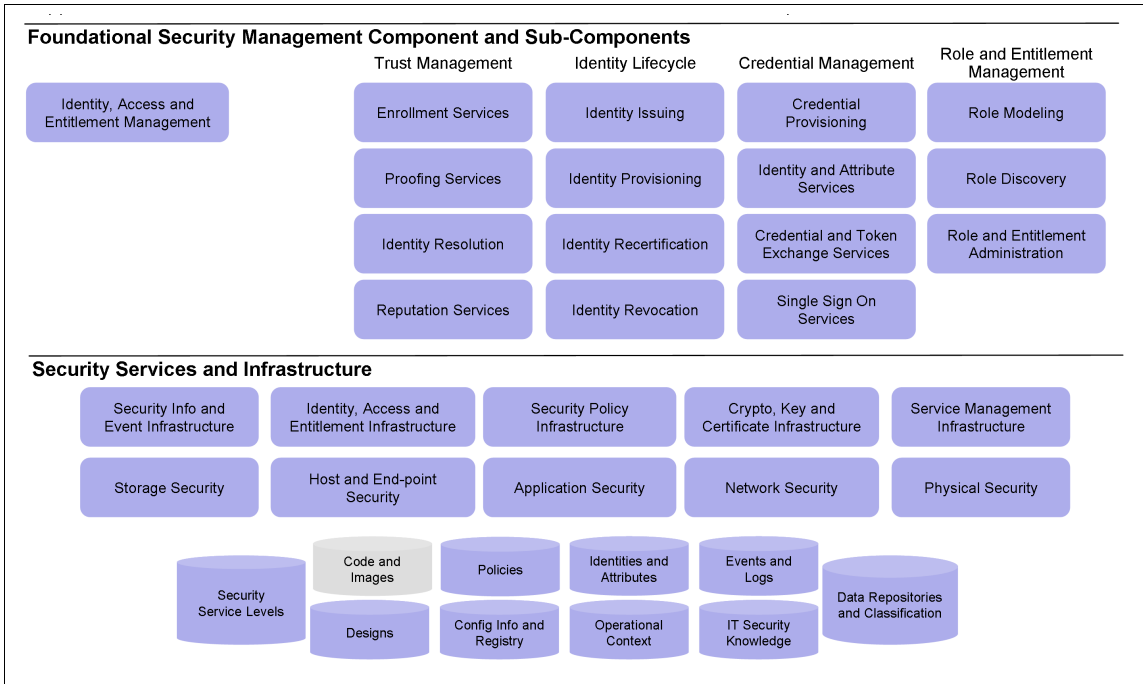


Figure 2-5 Identity, Access, and Entitlement Management subcomponents

Identity, Access, and Entitlement Management consists of the following subcomponent groups:

- ▶ Trust Management
- ▶ Identity Lifecycle
- ▶ Credential Management
- ▶ Role and Entitlement Management

These groups are explained in the next sections.

### Trust Management

Trust Management refers to the activities that are needed to improve the reliability of identity management systems to ensure that credentials are issued to the correct people.

### ***Enrollment Services***

Enrollment Services cover the act of collecting initial documentation from the person who wants to be issued a credential, including things like birth certificates and other source documents. It might also involve collecting biometric and biographic information.

### ***Proofing Services***

Proofing Services are the processes and technology for verifying all the information that is collected from the individual with the enrollment services. In addition to verifying information against authoritative sources, it might also include using identity analytics to detect fraudulent applications.

### ***Identity Resolution Services***

Identity Resolution Services cover the processes and techniques to identify multiple records for the same person, whether by accident or fraud, and to resolve them into a single record for a single person.

### ***Reputation Services***

Reputation Services involves tracking an individual's actions over time, collecting data about the opinions others have about those actions either from other individuals or rating systems, and publishing an assessment of the opinions either publicly or to the subject individual as a feedback mechanism.

## **Identity Lifecycle**

The Identity Lifecycle spans from the initial creation of specific events during the life of an identity to the final deletion of an identity. The key elements of the Identity Lifecycle are explained in the following sections.

### ***Identity Provisioning***

Identity Provisioning covers the processes and technology that is used to create the credential that is used when you issue an identity token (for example, a national ID card) and registering the credential to systems that must authenticate the credential.

### ***Identity Issuing***

Identity Issuing covers the processes and technology that is used to create the physical components of the credential and securely deliver it to the owning individual.

### ***Identity Recertification***

Identity Recertification refers to the processes and technology that are used to revalidate a credential that is already issued. In certain cases, this situation means that you update the credential itself. For example, a digital certificate has expired and another one must be issued. In other cases, the recertification involves reauthorization and presenting proofing materials again.

### ***Identity Revocation***

Identity Revocation covers the processes and technologies that are used to de-certify a credential so that it can no longer be used as an identity token. This situation can happen through normal expiration processes or be initiated by an outside trigger event. For example, a revoked digital certificate might be published on a certificate revocation list, which is checked by the identity infrastructure.

## **Credential Management**

Credential Management deals with the administration of credential information and related identity information. Besides the handling of credentials in electronic format, credential management also includes the administration of physical credentials, such as tokens or badges.

### ***Credential Provisioning***

Credential Provisioning covers the activation of the issued credential so that it can be used to validate an individual's identity, in addition to services for updating, deleting, and managing trusted identity credentials through the entire lifecycle.

### ***Identity and Attribute Services***

Identity and Attribute Services manage access to local user registries and databases that provide identity information. Typically, identity and attribute services are able to add and delete identity information in addition to reading it.

Identity and Attribute Services are used by authentication services when they evaluate user-presented authentication credentials and to build privilege credentials that are used by session management services. The privileges are typically based on attributes of a user that is stored in the Identities and Attributes security service, such as group membership, roles, and personal attributes.

Identities and Attribute Services that also manage the attributes about a user are sometimes referred to as Identity And Attribute Services (IdAS).

### ***Credential and Token Exchange Services***

Credential and Token Exchange Services combine token validation and issuance to convert one type of security token into another. Security tokens are validated in terms of signatures on the token, expected structure, and contents of the token. Token issuance involves creating a new, locally valid token that is based on the received, validated token. When this new token is returned to the original requestor, the process is referred to as a token exchange. The requestor is in effect exchanging the token that it received on a request for a new token that is locally valid.

### ***Single Sign-on Services***

Single Sign-on Services implement a set of protocols that are designed to remove the burden of repeating actions that are placed on the requestor. Typically, an identity provider can act as a proxy on a requestor's behalf to provide evidence of authentication events to third parties that request information about the requestor.

These identity providers (IdPs) are trusted third parties and must be trusted by both the person who originates the original request and the online service that allows the requestor to engage in sensitive or high-value transactions.

### ***Role and Entitlement Management***

Role and Entitlement Management embraces all functional services that relate to the grouping of identities and to the administration of access to information and resources at a group rather than an individual level.

### ***Role Modeling***

Role Modeling deals with the design of role structures to address requirements as they derive from the business and IT activities. The goal of role modeling is to reduce the complexity of actors by grouping them, which can result in the capability to provide and to restrict access to information and other resources more efficiently. This action is less error prone when you enforce a separation of duties.

### ***Role Discovery***

Role Discovery refers to the identification of roles and their respective entitlement. The necessary information about roles and entitlements can be gathered manually by observation and analysis of processes and interviews of the process actioner or process owners. Information can also be captured from systems that support the processes. User activity, to a certain extent, can be automatically analyzed and structured to derive roles and entitlement patterns.

## ***Role and Entitlement Administration***

Role and Entitlement Administration deals with the activities around maintaining and updating the role and entitlement structures. It is similar to the management of identities.

## **Security Services and Infrastructure components**

The following Security Services and Infrastructure components are key to effective Identity, Access, and Entitlement Management (depicted as blue-shaded objects in Figure 2-5 on page 59):

- ▶ **Security Information and Event Infrastructure**

Records of access attempts and whether they were granted is one of the most important records of activity for audit purposes, especially access records for privileged users. Policy enforcement points are responsible for generating appropriate audit records for these activities. These records are typically collected by a Security Information and Event Infrastructure for long-term tamper-proof storage, normalization, correlation with other events, and to provide appropriate evidence during audits.

- ▶ **Identity, Access, and Entitlement Infrastructure**

The Identity, Access, and Entitlement Infrastructure represents the Policy Decision Points and Policy Enforcement Points that make authorization decisions and enforce them during run time.

The Identity, Access, and Entitlement Infrastructure includes access control points to prevent unauthorized access to data, applications, and other IT resources both from a business operations perspective and from an IT administration perspective. These control points are driven by policies and entitlements that are defined in the Identity, Access, and Entitlement Management component in the Foundational Security Management layer.

The access control points rely on authentication mechanisms in the infrastructure and an identity management provisioning infrastructure that manages the accounts, passwords, public key certificates, and other materials that are needed for authentication.

The access control points are also the focal point for monitoring and enforcing segregation of duty policies as defined by the Identity, Access, and Entitlement Management component in the Foundational Security Management layer.

- ▶ **Security Policy Infrastructure**

The Security Policy Infrastructure is responsible for taking a common access control policy that is defined in the Security Policy Management system, transforming it into a format that the Policy Decision Point can interpret, and securely delivering it to the Policy Decision Point.

- **Cryptography, Key, and Certificate Infrastructure**

In many cases, the credentials that are used in an authentication request are signed or encrypted so that a Policy Decision Point can correctly validate the credentials. The Cryptography, Key, and Certificate Infrastructure can perform cryptographic operations and signature validation and creation as needed to process authentication requests.

- **Service Management Infrastructure**

Identity management processes in an organization help manage the entitlements to applications and data, typically using organizational roles as a basis for deciding who is entitled to which resources. The entitlements must be translated into specific credentials on target systems in the runtime environment so that the Policy Enforcement Points know which credentials to grant access and which to deny. The Service Management Infrastructure is responsible for interacting with the user repositories on target systems and creating and modifying the accounts on those systems so that the owner is granted the appropriate access based on his entitlements.

- **Storage Security**

The Storage Security infrastructure is responsible for protecting storage media from out-of-band attacks, such as theft of media, unauthorized duplication of media, or interception of traffic to and from the storage system. Storage Security relies on Identity, Access, and Entitlement Management to define and manage the administrators and the runtime systems that have access to the storage system.

- **Host and End-point Security**

Host and End-point Security is tightly integrated with Identity, Access, and Entitlement Management. Endpoint machines, by their nature, are often the initial point of contact with a user and are the first point that a user has the opportunity to authenticate to the IT environment. As a result, credentials that are established by the endpoint often must be propagated to back-end systems or translated into equivalent credentials that are used in back-end systems. Likewise, the endpoints become a key component for single sign-on services.



► Application Security

As part of their design, applications typically use a set of application-specific roles. These roles define who can interact with an application, and in what way, to access the various services that the application provides. The application platform is typically responsible for defining associations between the application-specific roles and the organizational roles that are managed by the Identity, Access, and Entitlement Management system. These associations are then translated into access control policies that the application platform uses to grant or deny access to the application at run time.

► Network Security

Granting and denying access to the network is a key component of Network Security. Network Security depends on the Access, Identity, and Entitlement management system to manage who is granted access to which parts of the network and to generate the necessary credentials and access control policies for the Network Security infrastructure to use at run time.

► Physical Security

Physical Security increasingly relies on logical access security to protect physical access. The most common examples include access control systems on doors, such as password keypads, biometric scanners, or badge readers. In many cases, these access control systems require that access is granted on a per-person basis. In these cases, the Physical Security systems rely on the Identity, Access, and Entitlement Management system to manage the identities and entitlements (who can access which parts of the physical facility) in an organization.

► Security Service Levels

The security service level agreements set objectives for managing access to key applications, data, networks, and physical facilities, in addition to the reporting and auditing requirements to demonstrate that the access controls are deployed and effective. Security service level agreements might also include provisions for various types of penetration tests of the access controls and performance metrics for the access control systems.

► Designs

Most IT-related designs in an organization define access control policies for the elements that they represent. These policies must be incorporated into the Security Policy Management system and represented as access control policies that the Identity, Access, and Entitlement Infrastructure services must be able to enforce.

IT designs and other business-oriented domain designs are often considered to be high-value assets and are subject to access controls and auditing. So the document management systems that are used to store these designs rely on the Identity, Access, and Entitlement Management system to define the policies about who can access which designs.

- ▶ Policies

One of the primary inputs into an Identity, Access, and Entitlement Management system are policies, which define the organizational roles and their entitlements to applications, data, networks, and physical facilities. The Security Policy Management infrastructure is responsible for the authoring processes for these policies, and the Identity, Access, and Entitlement Management system is responsible for translating access control policies into machine-interpretable formats that can be understood by the Policy Decision Points and Policy Enforcement Points.

- ▶ Configuration Information and Registry

Because the configuration management databases and registries for IT resources represent valuable knowledge that can be used in an attack, access to those resources is typically tightly controlled and made available only to a few privileged users.

- ▶ Identities and Attributes

The directories that contain information about employees in an organization and key attributes for them represent the primary data component for an Identity, Access, and Entitlement Management system. These directories are typically tightly integrated with human resources systems or are synchronized with them so that they always reflect the organizational structure for the enterprise. The Identity, Access, and Entitlement Management system relies on the directories when it maps organizational roles to application roles and other sorts of entitlements. Also, other repositories such as CRM databases (for customers) or procurement applications (for contractors) can provide information about people that require access to resources.

- ▶ Operational Context

Access control policies increasingly depend on information that is not available at run time. For example, an access control policy can grant access to a resource only if the requester is assigned to a unit of work that the resource is associated with, or it might grant access to a resource only during certain times of day or from certain locations. The Identity, Access, and Entitlement Management system must be aware of the Operational Context at run time to author policies that incorporate this runtime context.

- ▶ IT Security Knowledge

Defining appropriate access control policies to implement an organization policy requires a working knowledge of access control principles, such as granting of least privilege and how to combine entitlements when a person fulfills multiple roles in an organization. IT Security Knowledge is also important to choose appropriate Policy Decision Points and Policy Enforcement Points in an IT environment.

- ▶ Data Repositories and Classification

Data repositories are increasingly incorporating access control mechanisms to create an access control point as close to the data as possible. The classifications of the data in repositories must be available to the Identity, Access, and Entitlement Management system to define access control policies that are appropriate for the data classification.

## 2.2.5 Data and Information Protection Management

Data and Information Protection Management provides services that protect unstructured and structured data from unauthorized disclosure, modification, and loss, according to the nature and business value of information. It also provides usage and access monitoring and audit services.

Information technology today provides the core elements of most business processes: *transactions* and *data*. Both of these elements share a common quality: They involve facts and information. The transaction is the factual record that events occur, which produce data in the process. Taken a step further, the transaction is the record of a relevant event. Data involves the facts and information that are needed to conduct business or to make decisions. Data and Information Protection Management therefore validates and protects transactions and data in the organization to ensure that the data (which includes transactions) is complete, accurate, appropriately protected, and available.

Businesses are built on transactions that document exchanges or business agreements. As such, transactions represent the core element of the business. These transactions can be internal transactions between systems, or they can be external transactions with business partners, customers, or vendors. The ability to conduct these transactions is critical to the success and continuation of the business.

An organization produces and gathers other data as part of the business processes that are associated with maintaining the stream of transactions. The organization uses this data in the decision making process, making the data the core business knowledge of the enterprise. This data can contain intellectual property that gives the business a competitive advantage, or it can contain process-related information (and metadata) that is critical to business operations.

Figure 2-6 shows an overview of data and information protection management subcomponents and the related components from the Security Services and Infrastructure layer.

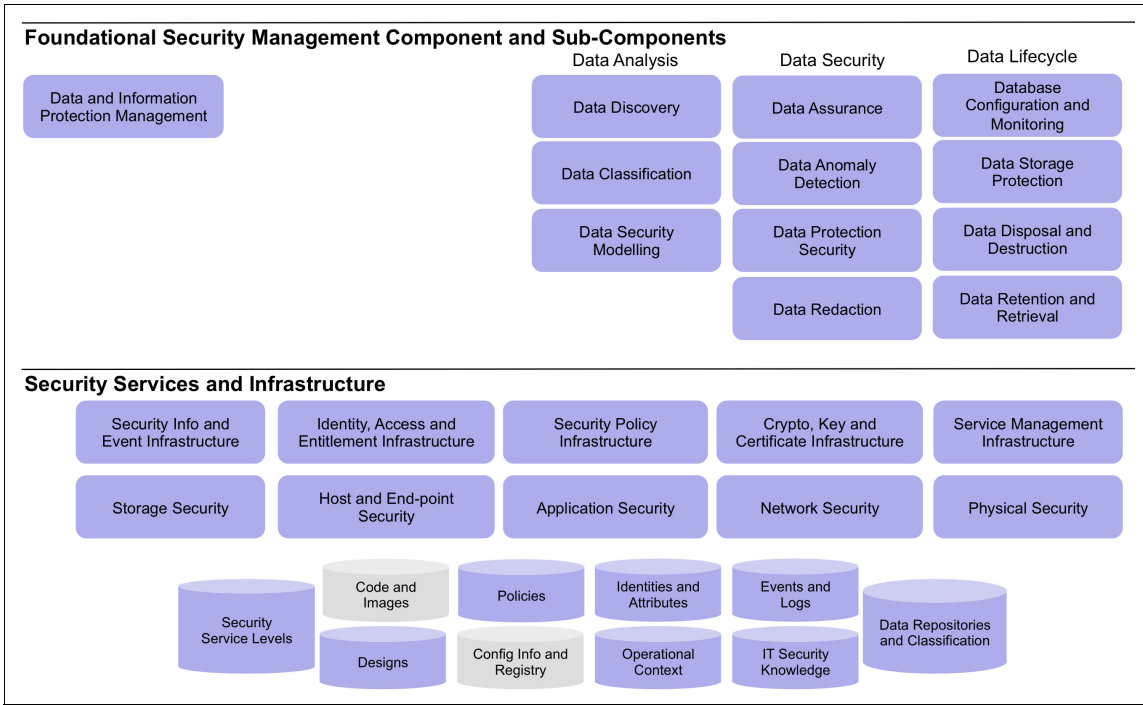


Figure 2-6 Data and Information Protection Management subcomponents

Data and Information Protection Management consists of the following subcomponent groups:

- Data Analysis
- Data Security
- Data Lifecycle

These groups are explained in the following sections.

## **Data Analysis**

The Data Analysis section focuses on the discovery, classification, and modeling of data in an organization.

### ***Data Discovery***

A crucial part of analyzing data is having an accurate inventory of the organization's data repositories and understanding the security risks that are associated with them. Data Discovery is the process of identifying all the data repositories in an organization and analyzing the schema and data values and data patterns to identify relationships between the database elements. An organization must know who is using data and how it is used, whether data is moving across boundaries (countries, business), or if it is being used for production or test.

Data Discovery looks at data relationships across repositories, understands how they relate to each other, and understands how the structured relationships are organized to represent business objects.

Data Discovery detects transformations and conditional logic that is applied to data as it is moved among repositories.

### ***Data Classification***

Data Classification refers to the tools and processes that are used to create a common set of semantic tags that are used by data modelers, data analysts, business analysts, governance stewards, and data architects. Data Classification is an also important factor for security and privacy policies.

Data Classification tools use rules and heuristics to examine logical data models from data repositories and associate business definitions with them.

In certain cases, business definitions relate directly to the format and constraints on the data (for example, the format of a telephone number). In other cases, there might be business-oriented definitions that are expressed in terms of the logical data model. For example, a high value customer might be defined as a customer who bought products more than a specified number of times in a specified time period.

Data Classification manages both lower-level, logical data classification and business level classifications.

At the business level, a collection of business classifications, their definitions, and how they relate to the underlying logical data model creates a common business vocabulary, which can be used across the organization to ensure that every part of an organization agrees on the definition of the term. This situation helps you to reduce confusion and miscommunication at the level of business discussions and also reduces interoperability errors across the IT organization.

A business vocabulary term might change over time and might have a significant impact on logical data models, database schema, and application logic. Data Classification tools can also enable data stewards to manage an orderly transition over time from one version of a business term to another.

### ***Data Security Modeling***

Data Security Modeling refers to activities performed by a data architect to define domain-specific information models, logical data models, and physical data models.

Data Security Modeling captures the constraints on data types that are defined by an organization or an industry standard. They are business-oriented constraints that enable interoperability between systems and organizations. For example, bank routing codes represent a numeric string that follows certain rules in its format and interpretation for routing inter-bank transfers. Another form of constraint can be privacy-related.

Logical data models are the semantic hub of an enterprise architecture. Logical data models are sometimes overlooked in the software development lifecycle, but they are increasingly important in the SOA context. A logical data model allows data architects to depict an overview of data entities in an application or an enterprise without having to look at overwhelming implementation details. Logical data models are often used as input into other enterprise architecture activities, such as defining message formats and service interfaces. The logical data model is also the starting point for transforming a domain model into a specific schema for a database instance.

Physical data models are database-specific models that represent relational data objects (for example, tables, columns, primary keys, and foreign keys) and their relationships.

Each of these layers of modeling can have security-related constraints that are attached to them that define requirements for confidentiality and encryption, access control, obfuscation, and redaction.

## **Data Security**

Data Security focuses on the operational usage of data at both the micro and macro level. Data Security provides a micro-level view of database systems (or instances) to protect the integrity of data. This view requires placing a value on data assets and implementing the appropriate security protection that is based on that valuation. This valuation involves standardizing configurations, processes, and practices for databases across an organization. Data Security also uses Data Discovery and Data Classification to know *how* the data is used (by what processes) and *what* the data is (by classification).

There is also the macro-level view of the data and database systems in the organization. This view includes not just the data itself but also the definition, reference, and metadata for that data. An enterprise view of data, how it is valued, protected, stored, and used is developed. Data is defined and linked across the enterprise, presenting a clear picture of the data and its usage. This subcomponent provides more than just a simple aggregation of the data because it involves a high-level structuring of the data.

Data Security is concerned with both data at rest and data in motion.

## **Data Assurance**

Data Assurance refers to tools and activities that can help you ensure that data is cleansed and standardized to a defined model before it is used. Data Assurance also tracks the origin of the data when it is received through logging and auditing capabilities. Data Assurance processes also provide a governance checkpoint for aggregation, redaction, and obfuscation requirements to ensure confidentiality and privacy.

## **Data Anomaly Detection**

Data Anomaly Detection describes the increasing protective measures that are available to detect and prevent fraud. Data anomaly detection and prevention techniques evolved rapidly over the last number of years with the usage of neural networks and data mining techniques.

Data Anomaly Detection ensures that organizations collect and gather information that is based on defined standards and that there is an overall enterprise approach to implementing fraud detection, correlation, analysis, and management of reports. Approaches should also be based on defined criteria and standards and ensure separation of duties and that there is access to dedicated technology and skills.

Organizations should integrate fraud detection into other processes, such as governance, incident management, and problem change management, use advanced authorization, information exchange with third parties, and a published fraud policy.

It is considered a preferred practice to provide the following items:

- ▶ Processes to enable fraud prosecution evidence capture and presentation
- ▶ Dedicated technologies and skills
- ▶ Awareness training for employees
- ▶ Awareness material for third parties
- ▶ Protection for employees who come forward with evidence of fraud
- ▶ Real-time response mechanisms to events
- ▶ Annual reviews of auditing process for fraud detection
- ▶ A comprehensive staff fraud management plan

### ***Data Protection Security***

Data Protection Security provides data integrity, encryption, authentication, authorization, and audit measures for data at rest and data in motion that uses security policy and crypto infrastructure services.

Data integrity measures provide for the detection that data changed without the changes being authorized.

Encryption ensures that data at rest and data in motion is correctly protected by using the crypto services that follow the requirements that are specified in the security policy.

Authentication and authorization provide assurances that the data is not disclosed to unauthorized entities or processes. Authentication processes also establish a clear audit trail about who or what process is granted access.

Audit measures allow tracking who or what process accessed what data at any moment in time. The audit measures also allow correct reporting in accordance with corporate governance, legal, and regulatory requirements.

### ***Data Redaction***

Data Redaction refers to a set of tools and methods for eliminating sensitive or confidential data from a data set that is based on policy rules before it is given to a receiver.

Data Redaction techniques can be applied both to unstructured data, such as a collection of word-processing documents, or structured data in databases.

Various techniques can be used in Data Redaction in addition to fully eliminating the data. For example, data can be partially obfuscated by masking out portions of the sensitive data. Data can be partially aggregated in ways that make it impossible to determine individual data records. In certain techniques, errors can be deliberately introduced into data in ways that preserve confidentiality while preserving the ability to perform statistically valid operations on the data.



Data Redaction techniques enforce access control security policies while they enable the release of related and relevant data.

### **Data Lifecycle**

Data Lifecycle looks at the security of data in any method and at any time in which it is stored, according to its lifecycle. It protects the confidentiality, integrity, privacy, and availability of data by addressing the long-term storage of the data and is concerned with controls around access to the data while it is stored. It addresses the quality of the data storage to make sure that there is not any degradation in the requirements for the storage lifecycle and data usage and access.

### ***Database Configuration and Monitoring***

Appropriate database configuration and monitoring ensure that information assets are protected according to their business criticality. The more critical the data that a database houses, the better the controls that are required to ensure its confidentiality, integrity, privacy, and availability. For example, a database that contains data for a non-critical business system has a different level of protection in comparison to one that houses the human resource information for its employees.

### ***Data Storage Protection***

Data Storage Protection refers to how information can be protected in storage, whether storage is a notebook, a desktop computer, a server or near line storage, an archive or auxiliary storage, or removable media.

Data Storage Protection ensures that there is an agreed upon organization-wide approach to protection, control of access to removable media, a defined and implemented policy about the protection of storage devices, the usage of encrypted file systems for data storage, interfacing into other threat management capabilities, such as Standard Operation Environments, database security, and systems integrity, and awareness campaigns that are aimed at ensuring compliance.

### ***Data Disposal and Destruction***

Data Disposal and Destruction refers to the tools and processes that are used to delete data from a system that is no longer needed and required by law or policy to be retained (the process when information reaches the end of its lifecycle and must be destroyed). Disposing of data that is no longer needed reduces data management costs. In certain cases, regulations require that data be disposed of after certain time periods or when certain criteria are met.

Data Disposal and Destruction processes can create a security risk if they inadvertently leave a way for the disposed data to be retrieved. Data Disposal and Destruction tools and processes must be designed to thwart likely threats to recovering the data, which is based on the value and sensitivity of the data and the techniques that an attacker might employ to retrieve the disposed data.

The techniques and processes for disposing of data are sometimes dictated by regulations and policy. For example, a regulation might require that data be overwritten a number of times with random information to reduce the possibility of retrieving it later.

Data Disposal and Destruction tools and processes must also preserve sufficient records to show that the disposal processes were followed.

### ***Data Retention and Retrieval***

Data Retention capabilities cover both *backup* and *archive* tools and processes. Backup refers to the tools and activities that are needed to restore service to a well-known point in the event of system or media failure. Archiving refers to the tools and processes that are used to remove transactions from an active system that is no longer needed, but that might need to be preserved for legal requirements.

Although backup techniques tend to apply to media or file-level activity, the archiving functionality often must be aware of transactions. For example, a complete record of a business transaction might require you to preserve data from multiple tables in multiple databases and might even require that you preserve various unstructured documents as well. Collectively, the set of structured and unstructured data that is needed to preserve a transaction is referred to as a *historical reference snapshot format*.

After they are archived, the snapshot files can remain on the local storage media or can be deleted. The organization controls how long an archive copy is retained; this period is called the *retention period*. The retrieval process locates the copies within the archival storage and places them into a designated system, which might be the active transactional system or a system that is specifically designed for displaying archived transactions.

Data Retention tools and techniques are an important component of a records management system that adds to these capability processes to manage decisions about what must be kept and in certain cases what must be deleted according to policy.

Data Retrieval refers to the security considerations around long-term data retrieval from storage or archives. It ensures that there is a well-defined, fully implemented approach and enterprise-wide standard and processes, separation of duties, audit capability, and an interface to other processes. It furthermore ensures that organizations maintain data recovery facilities and uses key retrieval for encrypted storage through the usage of long-term keys or key changes during data recycling.

## Security Services and Infrastructure components

The following Security Services and Infrastructure components are key to effective Data and Information Protection Management services (depicted as blue-shaded objects in Figure 2-6 on page 68):

- ▶ Security Information and Event Infrastructure

Interactions with databases and content repositories are one of the major sources of security events because they can create a log of data access attempts and logs of administrative activity by privileged users.

- ▶ Identity, Access, and Entitlement Infrastructure

The Identity, Access, and Entitlement Infrastructure translates the activity of privileged accounts to specific people who are responsible for data stewardship. In addition, database servers and content repositories are increasingly used to manage entitlements to access data. This component can help tie database interaction to specific individuals, which is becoming more important because of increased compliance initiatives.

- ▶ Security Policy Infrastructure

Data access entitlements that are enforced by database servers and content repositories must be consistent with other access control policies in the organization. Integrating database servers and content repositories with the Security Policy Infrastructure helps ensure this consistency. In addition, data retention policies, disposal policies, and other policies that are managed by data stewards should be authored, approved, and managed through a common Security Policy Infrastructure to ensure consistency with other security policies in the organization.

- ▶ Cryptography, Key, and Certificate Infrastructure

Database servers, content repositories, and archive media capture *data at rest* and are subject to security requirements to encrypt data in case the storage media is subject to out-of-band attacks, such as media theft, making the data and information protection management systems dependent on the Cryptography, Key, and Certificate Infrastructure.

- ▶ Service Management Infrastructure

Because data access management, data retention, and data disposal activities are often driven by regulatory requirements and are subject to audit, it is not sufficient to have the capability to perform the necessary actions. It is necessary to show that the responsible people configured the Data and Information Protection Management systems in accordance with the agreed-upon policy and taken responsibility for the actions of the systems that they configured. These activities require a robust Service Management Infrastructure to manage the work flow processes associated with these activities.

- ▶ Storage Security

In addition to cryptographic protection for data that is stored on storage media, more Storage Security measures might be needed to protect the media and storage systems from tampering, theft, and copying.

- ▶ Host and End-point Security

Host and End-point Security is necessary for good Data and Information Protection Management to prevent access to the database servers and content repositories through the file system in the operating system.

- ▶ Application Security

Application Security is important for Data and Information Protection Management because compromised applications might be able to access the database servers and content repositories using the credentials of the application and issue unauthorized queries to them.

- ▶ Network Security

Network Security is important to Data and Information Protection Management to protect data while it is in transit. Although message-level encryption and connection-level encryption can be used to protect data in transit, a secured network is important to prevent out-of-band attacks, such as copying traffic for later decryption, man-in-the-middle attacks, and DNS cache poisoning.

- ▶ Physical Security

Physical Security for the database servers and content repositories is important to prevent out-of-band attacks, primarily media theft.

- ▶ Security Service Levels

Security Service Levels can contain the agreed-upon data retention and disposal activities and the agreements about data access logging necessary for demonstrating policy compliance.

► Designs

Domain, logical, and physical data models for the organization are key designs that are used in various enterprise IT architecture activities, including capacity planning for storage, application design, and message format design.

► Policies

Data retention policies and data disposal policies are key policies in every IT organization. Furthermore, the policies that are enforced by database servers and content repositories to manage access to the data must be consistent with access control policies at other layers of the application stack.

► Identities and Attributes

Credentials that are used by administrators and users to access data must be associated with individuals so that accountability for data access and usage can be managed. Often, attributes of individuals dictate the subset of data that they are authorized to see. For example, a sales manager might be allowed to see only the sales data for the region that he manages.

► Operational Context

Increasingly, database servers and content repositories are required to be aware of the credentials that are used to access them and the credentials that originated the request so that the data access logs can be associated with a responsible individual. The database servers and content repositories often must log the transaction IDs or other unit-of-work identifiers for audit purposes.

► IT Security Knowledge

There are several areas of general IT Security Knowledge that are important to Data and Information Protection Management. For example, understanding the relative strength of encryption algorithms and key lengths is important when you determine encryption protection for sensitive data. Understanding the most common ways that data media are stolen is important in determining media protection.

► Data Repositories and Classification

The first step in protecting data and information is keeping accurate inventories of where all the database servers and content repositories are and understanding their value and sensitivity.

## 2.2.6 Software, System, and Service Assurance

Software, System, and Service Assurance addresses how software, systems, and services are designed, developed, tested, operated, and maintained throughout the software lifecycle to create predictably secure software. This component covers structured design, threat modeling, software risk assessment, design reviews for security, source code reviews and analysis, dynamic application analysis, source code control and access monitoring, code/package signing and verification, quality assurance testing, and supplier and third-party code validation.

The types of components that are required vary based on what parts of the software development lifecycle a company participates in and how the software, systems, and services are deployed. For example, the software could be developed internally or it could be purchased and installed on premise. It could also be provided by a public cloud provider. If the software is being developed internally (even if part of the development is outsourced), all of the subcomponents are applicable. When the software is purchased, the focus should be on the Lifecycle Management and Security Testing subcomponents, but it is still important to ensure that a software developer uses *secure design practices*. If an application or service is being provided in a public cloud, then the service provider should be responsible for most of the subcomponents, but it is still important to verify their security practices and review the results of the Security Testing processes.

**Further reading:** If you want to learn more about integrating secure engineering practices into the Software Development Lifecycle, see *Security in Development: The IBM Secure Engineering Framework*, REDP-4641.

Figure 2-7 shows an overview of the Software, System, and Service Assurance subcomponents and the related components from the Security Services and Infrastructure layer.

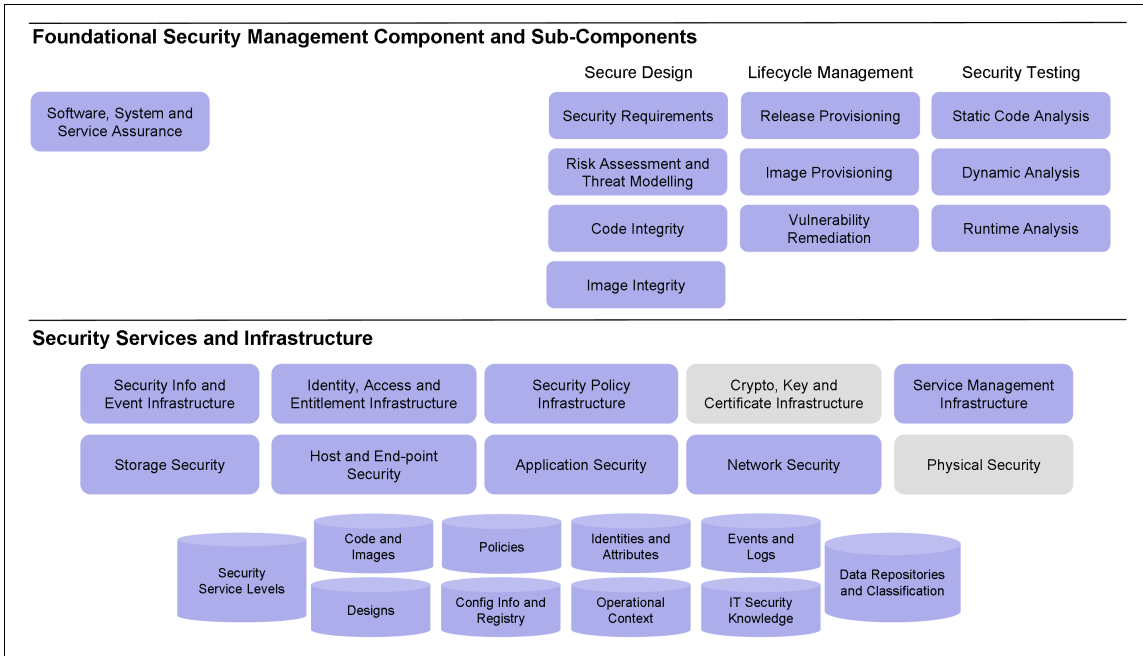


Figure 2-7 Software, System, and Service Assurance subcomponents

Software, System, and Service Assurance consists of the following subcomponent groups:

- ▶ Secure Design
- ▶ Lifecycle Management
- ▶ Security Testing

These groups are explained in the following sections.

### Secure Design

Secure Design includes the policies and processes that are required to both develop and deploy software, systems, and services that are secure by design.

## ***Security Requirements***

Just like functional requirements and performance requirements, security requirements are needed to help ensure that security is built into the application from the start. Security requirements define what security features are required and how existing features should be changed to include necessary security properties. The objective of security requirements is to help ensure that the application can defend itself from attack.

The following topics are examples of the security requirements that comprise the end-to-end security for an application:

- ▶ Auditing and logging
- ▶ Authentication and authorization
- ▶ Session management
- ▶ Input validation and output encoding
- ▶ Exception management
- ▶ Cryptography and integrity
- ▶ Data at rest
- ▶ Data in motion
- ▶ Configuration management

## ***Risk Assessment and Threat Modeling***

Threat Modeling allows development groups to identify potential risks or attacks against an application even before it is built and to decide about how to address these risks. Once identified, threats are ranked in importance and addressed according to a risk profile. Some threats should be addressed in the internal design of the component, product, or solution; however, some threats can be addressed by correct configuration and integration, or might require additional components or management processes to adequately control risks. In many, if not all cases, there can be residual risk in deploying and operating the components, products, and solutions.

## ***Code Integrity***

Code Integrity refers to protecting assets that are used to build and run application object code to ensure that what is delivered to service management for deployment was not tampered with or incorporated any unknown source code.

Code Integrity encompasses confidentiality of the source code from competitors and other unauthorized people. Code Integrity also ensures that all the correct licenses were obtained for the running instance of the code and ensures compliance with any development team restrictions (for example, *clean room* rules might need to be followed to protect against charges of reverse engineering).



### ***Image Integrity***

Image Integrity covers the entire runtime stack, from operating system to middleware components and application platforms that are needed to run the application or service. Images might include definitions of runtime dependencies that are assembled during the deployment process, or an image might be an entire pre-built software stack that is packaged as a virtual machine image.

In the case of virtual machine images, image integrity refers to the tools and processes to track the provenance of all the software components that are included in the image. Image Integrity also ensures that the image was not tampered with after it was assembled.

### **Lifecycle Management**

Effective Lifecycle Management is required to make sure that software, systems, and services are deployed securely and any vulnerabilities that are detected are remediated as quickly as possible.

### ***Release Provisioning***

Secure provisioning ensures that handing over code to release management for installation and configuration of the dependent software infrastructure is done in accordance with security policy and, in certain cases, per contract with the customer. For example, Release Provisioning might include a mapping of organizational roles and individuals to application-defined entitlement roles to ensure that the correct people in an organization are granted access to the correct application roles. Release Provisioning might also dictate security requirements for the database middleware to define requirements for protecting data at rest.

There should also be a direct link to Change and Release Management, which is a subcomponent of IT Service Management. Change and Release Management provides standard processes for upgrading deployed software components and the deployment of new software components.

### ***Image Provisioning***

Image Provisioning manages access to the image contents. For example, image administrators might not be authorized to see confidential data or code inside the image. Image Provisioning also manages access to the image for deployment, defining who can access and deploy instances of the image in a production environment.

Finally, Image Provisioning might impose deployment restrictions, especially security-related restrictions, on the service deployment processes. For example, an image might have a requirement that it is not deployed in a DMZ, but only behind strictly controlled firewalls. Or an image might have a requirement to not be co-hosted with images from any other company.

### ***Vulnerability Remediation***

When a vulnerability is detected and validated in an application, there should be a defined process incident response that includes providing a fix for that vulnerability. The incident response process should also include alerting other application teams that might be affected by the vulnerability.

### ***Security Testing***

There are different methods for analyzing applications to locate vulnerabilities that could be exploited. All of these methods should be used when you develop applications. When you use third-party applications and there is no access to source code, then both the dynamic and runtime analysis should still be used.

### ***Static Code Analysis***

Static Code Analysis refers to the tools and processes that are instituted by a software development team or a build team to examine all the artifacts and components that are used to build an application. The analysis looks for security vulnerabilities and poor coding practices that can create security, performance, or other problems.

Static Code Analysis usually refers to automated tools that scan source code and report on potential problems. But Static Code Analysis can also include design model reviews and scanning, in addition to manual inspection of application artifacts.

## ***Dynamic Analysis***

These tools perform an analysis of the application as a *black box*, without knowing its internal operation and source code. Dynamic Analysis tools automatically map the application, its entry points and exit points, and attempt to inject input, which either breaks the application or subvert its logic.

Dynamic Analysis can be extended to provide better accuracy and coverage using a hybrid analysis approach. Although a Dynamic Analysis scan relies mostly on a server response to determine whether a vulnerability exists, a hybrid analysis can scan the internal actions and structure of the web application. The result is scans that are complete, which can also identify more complex vulnerabilities and report the exact location of the vulnerability in the source code.

## ***Runtime Analysis***

Runtime Analysis, or *software profiling*, refers to the ability to observe a running software system and analyze its behavior to detect vulnerabilities in the code. This approach provides continual monitoring of the software, whereas static code analysis and dynamic analysis provide a status of the software at a point in time.

Although Runtime Analysis is often used to look for problems with memory usage, network usage, or other runtime resources, runtime analysis can also be used to identify potential security problems. For example, Runtime Analysis can highlight how an application fails to properly handle malformed messages that result in a failure to release allocated memory.

Runtime Analysis is an *internal view* of the running application, whereas Dynamic Analysis tests a running application by interacting with it from an *external perspective* in the same way that user or client software interacts with it.

## **Security Services and Infrastructure components**

The following Security Services and Infrastructure components are key to effective Software, System, and Service Assurance (depicted as blue-shaded objects in Figure 2-7 on page 79):

- **Security Information and Event Infrastructure**

When you plan the deployment of an application, the security-relevant events that it might generate must be planned for in the Security Information and Event Infrastructure. IT operations must know how to enable the application-specific event logging and understand where the events are stored. IT operations must also incorporate the application-specific logging in to their Security Information and Event Infrastructure and understand how to recognize potential security incidents from the event stream.

- ▶ Identity, Access, and Entitlement Infrastructure

Control of access to source code, images, and running applications must be tied to specific individuals by associating credentials with individuals and associating organizational roles with the management infrastructure roles and application-defined roles.

- ▶ Security Policy Infrastructure

Security policies that regulate how applications are deployed into an environment and how machine images are deployed into a virtualization platform can be managed by a Security Policy Infrastructure to ensure consistency across the organization. Access control policies to applications and images should be coordinated with other access control policies. Security policies (or the derived company standards and guidelines) should describe how operating systems and middleware should be configured.

- ▶ Service Management Infrastructure

Assurance activities define deployment and access requirements for applications and images that must be used and implemented by the release and deployment processes in the Service Management Infrastructure. Therefore, there must be coordination between development and operations to ensure that operations know how to implement the requirements that are defined by development.

- ▶ Storage Security

Applications define their dependency on storage infrastructure, and storage infrastructure components can be included in a virtual machine image. In both cases, the definitions might impose security requirements on the storage infrastructure, including requirements to encrypt storage media, locate it in a physically secure environment, and maintain data for a specified retention period.

- ▶ Host and Endpoint Security

Applications typically have limited awareness of the host environment and rely on security measures on the host to protect the application from out-of-band attacks. For example, it is the responsibility of Host and Endpoint Security to ensure that there are no processes on the host machine intercepting traffic between the application and its clients.

- ▶ Application Security

Although secure coding practices, static analysis, and secure design practices can limit the vulnerabilities in an application, the applications typically rely on Application Security enforcement points to help detect and prevent attacks such as cross-site scripting and SQL injection.

- Network Security

Applications have dependencies in the Network Security infrastructure to make certain that ports are available for remote connections and to ensure the appropriate isolation of network traffic. Certain application-layer attacks can be detected and prevented through deep packet inspection and other types of network traffic analysis.

- Security Service Levels

Government agencies and companies are starting to require assurances that software code is free of viruses, malicious coding, vendor or programmer created back doors or trapdoors (front and back), and other types of security vulnerabilities, which are considered a type of security service level for the software.

- Code and Images

Application Code and Images are the target resources that are protected by software, server, and security assurance.

- Designs

The application architecture that is represented in the software designs is the first line of defense in software security. Equally important, the application designs represent the formal definition of what the software does and delivers and are part of the provenance of a software application. Good software provenance should be able to trace a chain of activity from the running application back to the design that it implements.

- Policies

There are various policies that affect software assurance and image integrity. Applications define sets of roles that dictate which features are accessible to which people. These roles must be mapped to organizational roles by using an access control policy specific to the application.

Likewise, security policies must define who has the authority to instantiate which virtual machine images under which circumstances. The security policies must also define where in the virtual environment these images can be present. For example, a security policy might dictate when virtual machine images must be placed on a separate virtual network from other images.

- Identities and Attributes

Because applications are typically developed independently of any particular organization, they define access control mechanisms in terms of application-specific roles. These application-specific roles must be mapped to the organizational roles, which require an understanding of the directory information available about people and their credentials.

- ▶ **Operational Context**

Applications often rely on transactional context that comes from outside the application's environment. For example, an application might need to send SNMP events to a central management infrastructure, which must be defined to the application.

- ▶ **IT Security Knowledge**

An understanding of the types of attacks that applications are typically subject to is important in planning application architecture and design and is crucial to static code analysis. Other types of industry knowledge, such as the most common programming errors that lead to security vulnerabilities, are also important.

- ▶ **Data Repositories and Classification**

Virtually every application or web service relies on some sort of storage infrastructure for structured or unstructured data. These infrastructures are typically defined at deployment time and must be registered with a data repository catalog and classified according to organizational policy to ensure that they are adequately protected.

## **2.2.7 Threat and Vulnerability Management**

Threat and Vulnerability Management provides services that can help determine security threats and identify vulnerabilities in deployed systems, collect security-related information from various internal and external sources, and determine the appropriate response.

Figure 2-8 shows an overview of the Threat and Vulnerability Management subcomponents and the related components from the Security Services and Infrastructure layer.

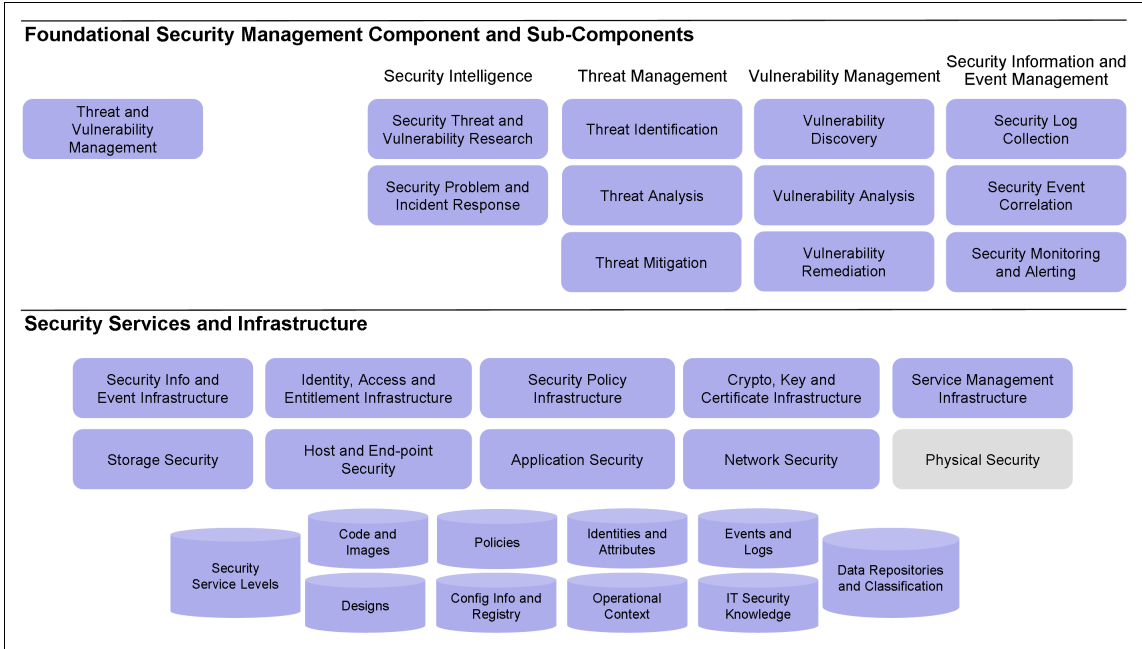


Figure 2-8 Threat and Vulnerability Management subcomponents

Threat and Vulnerability Management consists of the following subcomponent groups:

- ▶ Security Intelligence
- ▶ Threat Management
- ▶ Vulnerability Management
- ▶ Security Information and Event Management

These four groups are explained in the following sections.

### Security Intelligence

Security Intelligence provides security knowledge about threats and vulnerabilities.

### ***Security Threat and Vulnerability Research***

Security Threat and Vulnerability Research represents the ability to collect, analyze, and disseminate information as it pertains to computer security from reviewing and tracking a range of available information sources on potential threats and potential vulnerabilities to determine the applicability to an organization's IT environment.

In a more sophisticated execution, Security Threat and Vulnerability Research also includes the detailed observation, manipulation, and analysis of the behavior of *threat agents* and of the composition of *vulnerability conditions* in attack scenarios to synthesize, create, and provide respective knowledge about potential future attacks from collected data. It takes into account external, situational awareness, identifies and examines possible new attack patterns, and monitors long-term trends that might lead to specific new threats against the security of information assets.

People and processes that are associated with this component are also responsible for gathering awareness of future potential threats and vulnerabilities to the facilities from law enforcement agencies, regulatory agencies, and industry trade groups.

### ***Security Incident and Problem Response***

Security Incident and Problem Response provides support to the related IT Service Management functions *Incident Management* and *Problem Management* by providing security expert knowledge about identified attacks and security-related anomalies and by recommending respective actions to manage security incidents and problems to closure. It embraces security incident containment, security incident recovery, root cause analysis, security problem analysis, and security problem resolution.

### **Threat Management**

The Threat Management services deal with the identification, understanding, and counterfighting of specific threats that might exist for an IT environment.

A *threat* is the intention of a *threat agent* to perform a *threat action* to exploit a specific vulnerability. Only the occurrence of both threat and vulnerability together define the likelihood of a risk. If either threat or vulnerability does not exist, that risk has a likelihood of zero (there is no risk).



### ***Threat Identification***

Threat Identification embraces activities that help you discover actors and actions in the IT environment that might have a harmful effect on IT assets and the information that is stored and processed on them. Threat Identification can be performed purely manually, but today it can usually be based on the automated recognition of deviations from the usual operations in an IT environment. Any discovered anomalies can then be examined for their threat potential.

### ***Threat Analysis***

Threat Analysis is the continuous examination of available information that is related to *threat agents*, often called attackers, and their possible *threat actions*, the actual attack, to evaluate the severity of an identified threat, for example, that is based on the potential occurrence of an attack because of the general awareness of the attack vector and on the presumed attractiveness of an organization as an attack target in the view of an attacker.

### ***Threat Mitigation***

Threat Mitigation embraces efforts that are taken to influence either the threat agents or to manipulate the threat actions to reduce the severity of a threat. The usual efforts that are taken include, for example, declaring sanctions and disciplinary actions to threat agents upon discovery of their threat actions or even their planning of such threat actions, and the deployment of measures that negate their actions or identify and deviate them away from a vulnerability. Threat mitigation can consist of detective controls, such as the deployment of malware detection, intrusion detection, and honeypots.

## **Vulnerability Management**

The Vulnerability Management services deal with the discovery, understanding, and reduction of specific vulnerabilities that might exist for an IT environment.

A vulnerability is a weakness that can be exploited to compromise security.

### ***Vulnerability Discovery***

Vulnerability Discovery deals with the detection of vulnerabilities. Besides the application of holistic security thinking, well-known methods for Vulnerability Discovery include the following items:

- *Dynamic code analysis* to assess applications for vulnerabilities that might be exploited from an application user's perspective. To discover more about dynamic code analysis in relation to the Software, System, and Service Assurance subcomponent, see "Dynamic Analysis" on page 83.

- ▶ *Network vulnerability scanning* to probe operating systems, databases, middleware, and firewalls, which protect all deployed IT services from vulnerabilities that are accessible from the internet. The difference from dynamic code analysis is that network vulnerability scanning focuses more on off-the-shelf software packages, whereas dynamic code analysis focuses mostly on custom-built applications.
- ▶ *Security healthchecking* to check systems with scripts or through a local agent from the inside and assess the configurations of local and network services of operating systems, databases, middleware packages, and applications for errors that could lead to potentially exploitable vulnerabilities.
- ▶ *Ethical hacking* to perform simulated attacks against a part of or the entire IT environment by applying human creativity and out-of-the-box thinking, and by using a combination of automated discovery, probing and exploit tools, and manual or custom-scripted security tests. Such attacks can vary in scope, time, and resourcefulness, and in the provision of inside knowledge and access rights to simulate different attack scenarios. Providing no inside knowledge is considered a black box test, whereas providing the testers with background information about the design and architecture is considered a white box test.

### ***Vulnerability Analysis***

Vulnerability Analysis covers the actual verification of vulnerabilities by eradicating false positives, and further covers the rating of such vulnerabilities in terms of criticality (for example, based on their ease of discovery and the complexity of their exploitability by attackers, and on the level of the resulting compromise of a tested system or environment).

### ***Vulnerability Remediation***

Vulnerability Remediation encompasses the combination of deterrent, preventive, detective, and corrective security controls to mitigate identified and verified vulnerabilities. The most commonly applied mitigation approaches to eliminate a vulnerability include the following measures:

- ▶ Fix the related code by patching.
- ▶ Change the configuration of the vulnerable service.
- ▶ Apply more preventive security controls, such as firewall and intrusion prevention systems with virtual patching capabilities.
- ▶ Employ more corrective measures, such as increased frequency of system checks, data backups for quicker recovery, and enhanced emergency response procedures.

## **Security Information and Event Management**

After the event data is centrally collected, it can be consolidated and structured and combined and correlated to derive more meaningful and human-understandable security information.

### ***Security Log Collection and Normalization***

Security Log Collection and Normalization refers to the ability to collect security-related events from various collection points in the IT environment, usually in the form of system, network, and security log and alert data, and to store them in a structured way to have a redundant copy (alongside the logs on the originating systems) to retrieve and analyze them during security incidents and problems in case the logs on the originating systems are compromised.

### ***Security Event Correlation and Normalization***

Security Event Correlation and Normalization builds upon Security Log Collection. After the log data is centrally collected, it can be consolidated and structured, standardized, combined, correlated, and normalized into security events to derive more meaningful and human-understandable security information.

### ***Security Monitoring and Alerting***

Security Monitoring and Alerting refers to all activities related to the ongoing and frequent observation of the technical infrastructure for deviations from the standard operation, which confirm or at least indicate an impact on security.

## **Security Services and Infrastructure components**

The following Security Services and Infrastructure components are key to effective Threat and Vulnerability Management (depicted as blue-shaded objects in Figure 2-8 on page 87):

- ▶ **Security Information and Event Infrastructure**

The Security Information and Event Infrastructure collects security log data from various agents that are deployed throughout the IT environment. It can create events and incidents that can be combined with other events and incidents in a standardized format by consolidating, classifying, and correlating all collected information. The aggregation of security logs and the subsequent derivation of security information is essential for all vulnerability-related services within the Threat and Vulnerability Management discipline. The large amount of data that is collected over time allows the Security Information and Event Infrastructure services to analyze trends of attack patterns as part of the security intelligence services and thus can also help to derive probabilities of threats.

- Identity, Access, and Entitlement Infrastructure

The Identity, Access, and Entitlement Infrastructure is used by the Threat and Vulnerability Management services to further analyze and tie events to identities and entitlements to confirm whether events relate back to authorized activities or whether they occurred from unauthorized or even malicious activities.

- Security Policy Infrastructure

The Security Policy Infrastructure can help Threat and Vulnerability Management services to eliminate or reduce *false positives*. A false positive is an event that, from a pure technical security perspective, is considered a threat. For example, a particular event is granted a *policy exception* because a business application requires a specific network port to be used, although this port is known to be used for attacks. By consolidating with the Security Policy Infrastructure, this particular event is no longer flagged as a security event.

- Cryptography, Key, and Certificate Infrastructure

Communication between distributed infrastructure components for Threat Management, Vulnerability Management, and between systems and the Security Information and Event Management infrastructure components is subject to encryption and secure authentication using certificates. Also, the log data might have to be encrypted or signed to protect against manipulation, so that Threat and Vulnerability Management services depend on the Cryptography, Key, and Certificate Infrastructure.

- Service Management Infrastructure

Threat and Vulnerability Management services operate within agreed-upon service management infrastructures and must also use the services that are provided by that infrastructure. For example, performing vulnerability discovery activities and transferring evidence from the testing environment are typical operations that must be performed in line with Change Management and thus use the Service Management Infrastructure.

- Storage Security

Storage Security provides logging and alerting functionality that can be used and examined either directly by Threat and Vulnerability Management services or indirectly by the Security Information and Event Infrastructure. Storage Security can also employ dedicated monitoring agents that can provide a more comprehensive functionality than basic logging and alerting. Storage Security can also provide masking and filtering functionality that comes with most database products to allow improved vulnerability discovery and mitigation.

► Host and Endpoint Security

Like Storage Security, Host and Endpoint Security can provide security functionality that allows the Threat and Vulnerability Management services to identify and remediate vulnerabilities either proactively or reactively. Examples of such functionality include malware scanning and remediation software, host intrusion detection and prevention systems, and security healthchecking software. Besides deploying more software, many basic operating systems and middleware components provide configuration options to limit security vulnerabilities, or even the potential for future vulnerabilities by configuring stricter values and thus hardening systems against attacks.

► Application Security

Application Security provides options for security configurations and might include security defense mechanisms such as input revalidation to close known attack vectors.

► Network Security

Network Security provides filtering, monitoring, alerting, and discovery functionalities by using firewalls, routers, network device logging, network intrusion detection and prevention systems, and network protocol and application protocol vulnerability scanners.

► Security Service Levels

The Security Service Levels provide the operational background for the security policies. This information helps the Threat and Vulnerability Management services to better implement the required level of protection. Also, as Threat and Vulnerability Management services often operate using high privileges and access rights in the IT environment, it is important that these services follow the appropriate policies that are set for their activities.

► Code and Images

Code and Images are constantly examined by Threat and Vulnerability Management services for identified vulnerabilities within them.

► Designs

Designs are an important reference for Threat and Vulnerability Management services, as you can use them to derive potential attack and testing scenarios for vulnerability discovery and threat analysis services.

- Policies

Policies must be adhered to by Threat and Vulnerability Management services, especially as these services operate with high, sometimes ultimate, privileges in the IT environment. Because certain Threat and Vulnerability Management services emulate attacks, the approach and limits of such activities must be strictly regulated in policies before they can be run.

- Configuration Information and Registry

The configuration management database and the registries of IT resources are used to store security settings and important asset information. This information must be available for a root cause analysis as part of a security threat investigation or a vulnerability examination as part of a security vulnerability assessment.

For example, it is essential to check the configuration information to examine the reason for an identified dangerous configuration. It might have been introduced as part of an approved configuration change or it might have been introduced as part of a malicious system attack. By examining the recorded configuration information that is stored in the configuration management database, security administrators are able to determine either regular behavior or malicious intent and act.

Likewise, a vulnerability examination can greatly benefit from configuration and registry information because this information can be helpful to determine the number and location of systems that are exposed to a specific vulnerability.

- Identities and Attributes

Identities and Attributes are assessed by Threat and Vulnerability Management services as part of vulnerability discovery and incident and problem response tasks.

An example for the discovery of a security problem with an abuse of identity can be identified by cross-checking the user activity on systems with the attributes of the corresponding identity. In a case where the stored identity information for a particular user ID shows an attribute of *revoked*, and there are still activities that are performed on systems in the context of this particular user ID, there is a high likelihood that this user ID is used in a malicious context.

- Operational Context

The Operational Context can help clarify whether an activity and its related events are harmless and intended or unplanned and potentially malicious. Thus, the Operational Context must be reviewed by the Threat and Vulnerability Management services to come to a correct conclusion. For example, a discovered suspicious activity, such as an internal network scan, might be related to authorized changes or problem determination activities.

Because the Operational Context clarifies the legit intention, this event does not represent a potential attack.

- ▶ IT Security Knowledge

A deep and broad IT Security Knowledge is of key importance to Threat and Vulnerability Management. The type of knowledge that is required includes a deep technical understanding of platform-specific security functions and the ability to understand the performance of security attacks in a step-by-step manner. Besides the technical knowledge, it is also required that security experts that work in Threat and Vulnerability Management are always up to date on new technologies so that they are able to identify potential new types of threats that might come with these innovations. Alongside of the IT Security Knowledge, it is also necessary to have skills in using the various security analysis and testing tools.

Finally, the provision of these services requires the ability to understand new security attack patterns and also the skills to efficiently keep up to date on newly discovered threats and vulnerabilities.

- ▶ Events and Logs

Event and logs are the most essential objects for the Threat and Vulnerability Management services, as they contain all the collected log and event information necessary to identify actual attacks.

- ▶ Data Repositories and Classification

Understanding of the Data Repositories and Classification is required by the Threat and Vulnerability Management services to allow thorough analysis of potential threats and targeted creative thinking about potential vulnerabilities and related attack patterns.

## 2.2.8 IT Service Management

IT Service Management provides the process automation and workflow foundation for all IT delivery activities, including security management. In particular, Change Management and Incident Management processes play a significant role in security management.

**Scope of this description:** This section is not intended to be a complete description of all IT Service Management domains. This section focus on the key IT Service Management components that contribute to security.

Figure 2-9 shows an overview of the IT Service Management subcomponents and the related key components from the Security Services and Infrastructure layer.

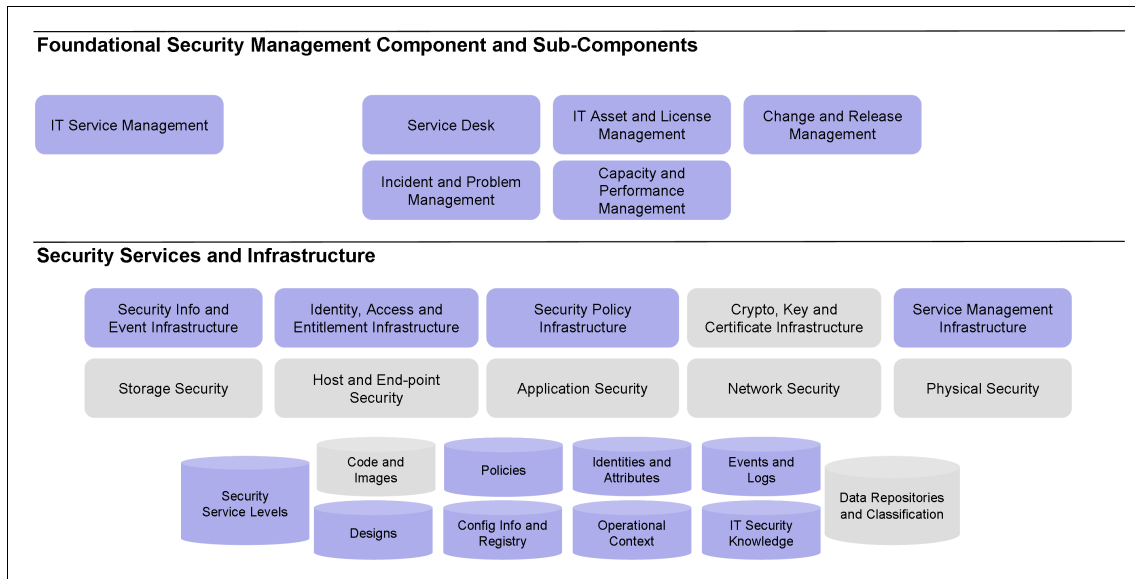


Figure 2-9 IT Service Management subcomponents

IT Service Management consists of the following subcomponents:

- ▶ Service Desk
- ▶ Asset and License Management
- ▶ Change and Release Management
- ▶ Incident and Problem Management
- ▶ Capacity and Performance Management

These subcomponents are explained in the following sections.

## Service Desk

Service Desk refers to the *single point of contact* (SPOC) for all IT Service Management related matters where all service management functions are coordinated. In particular, the Service Desk provides a ticketing and tracking functionality for service delivery activities, including activities in the security management area.

## Asset and License Management

Asset and License Management covers a set of capabilities to monitor deployed IT assets from a financial, compliance, and inventory perspective.



From a software perspective, Asset and License Management includes license management, certain aspects of configuration management (for inventory management purposes), and reporting for regulatory purposes. License management maintains an inventory of deployed software, measures usage activity, and manages entitlements to licensed software. It checks for adherence to license use requirements, summarizes software use for planning purposes, and helps with user chargeback activities.

Hardware asset management includes the physical characteristics of deployed hardware components in the IT environment, such as their make and model numbers, serial numbers, physical locations, and their role and placement in the network. Hardware asset management involves tracking regular maintenance of the hardware assets, tracking history of physical failures, and so on. Hardware asset management is often also involved in recording and tracking the financial view of the asset.

## **Change and Release Management**

Change and Release Management covers the standardization of methods and work processes to manage changes to the configuration of deployed IT assets and to the upgrade of existing deployed software components and the deployment of new software components. The goals of this standardization are to minimize disruption of service and to ensure that software and hardware components are not deployed in ways that compromise any security or integrity aspects.

## **Incident and Problem Management**

Incident and Problem Management handles the methods and processes that are used to restore service from any sort of disruption because of incidents and problems. An *incident* is considered a single event or a group of events that occur in parallel or in a short period in time and that trigger a negative impact on the level of service. A *problem* is considered a result of repetitive incidents of the same or a similar pattern, or as a result of an elevation of an incident because of its continued significant impact on the level of service or because of the increased efforts that are required to return to normal operations.

From a security perspective, the incidents and problems that are classified as *security incidents* and *security problems* require support from security incident and problem support or security emergency response teams.

## Capacity and Performance Management

Capacity and Performance Management deals with the planning, provisioning, and optimization of IT resources that are required for the IT services. In a narrow sense, this component mostly refers to details such as processing power and memory, system backup and archive storage, and network speed or bandwidth. In a wider context, Capacity and Performance Management can also include human resources and physical asset resources, such as floor space in a data center. This area is important to security, as the security services and their related infrastructure components that are deployed in an IT environment can use a significant amount of resources, and thus can impact performance.

All too often, such an impact is ignored or not properly examined when security is not embedded in the planning of IT services from the start and also when the addition of new security controls is considered (for example, as a result of a security incident remediation).

## Security Services and Infrastructure components

The following Security Services and Infrastructure components are key to effective IT Service Management (depicted as blue-shaded objects in Figure 2-9 on page 96):

- Security Information and Event Infrastructure

The Security Information and Event Infrastructure is used by the IT Service Management services to monitor and observe changes in security-related assets that might result or relate to change and release execution or trigger incidents and problems. These events, when confirmed, can become security incidents and security problems and are sent to Threat and Vulnerability Management services for resolution.

- Identity, Access, and Entitlement Infrastructure

The Identity, Access, and Entitlement Infrastructure is used by the IT Service Management services to assign potential actioners for change and release, incident and problem, and capacity and Performance Management activities on systems.

The Identity, Access, and Entitlement Infrastructure is also used by IT Service Management to review and authorize access to the components of the IT environment because IT Service Management is the owner of and thus overall is responsible for the IT services.

- ▶ **Security Policy Infrastructure**

The Security Policy Infrastructure is used by IT Service Management services to check and verify security requirements that must be adhered to (for example, under which conditions and in which timeframes) to avoid negative impact during changes and releases and during incident and problem handling activities.
- ▶ **Service Management Infrastructure**

The Service Management Infrastructure provides the overall ticketing and tracking, and progress and status reporting system for all IT Service Management services.
- ▶ **Security Service Levels**

The Security Service Levels are a subset of the overall IT service levels that IT Service Management must deliver and report on. The IT Service Management services (in particular the service desk) must consider the potential impact to the Security Service Levels by other service activities when you plan and schedule them.
- ▶ **Designs**

Designs are important to IT Service Management services to understand potential impacts to the services. For example, planned and accepted changes to one component can have possible effect on other components, which is of particular importance for the capacity and Performance Management services.
- ▶ **Policies**

Policies can help IT Service Management to identify and confirm security requirements that must be considered during any of the IT Service Management services activities.
- ▶ **Configuration Information and Registry**

The Configuration Information and Registry is mostly used and updated as a consequence of IT Service Management services and must be kept up-to-date in line with their activities to represent an accurate state of the deployed configurations.
- ▶ **Identities and Attributes**

Identities and Attributes feed directly into the Identity, Access, and Entitlement Infrastructure, which is used by the IT Service Management services.

- ▶ Operational Context

As with designs, IT Service Management services use and update the Operational Context for the IT environment in line with the change, release, and other IT Service Management activities.

- ▶ Events and Logs

Event and logs are created alongside the activities of IT Service Management services, and thus the event and log items are used to check and validate the actual progress of initiated activities.

- ▶ IT Security Knowledge

The IT Security Knowledge that is required for IT Service Management activities consists mainly of the general understanding of security matters and of the security awareness that is required to prioritize and sufficiently consider security in general IT Service Management activities. For example, incident and problem management must have a sufficient security understanding to identify that an incident or problem might be related or have an impact on the security posture.

## 2.2.9 Physical Asset Management

Physical Asset Management provides awareness of the location and status of physical assets and awareness of Physical Security controls and coordinates the security information for physical systems with the IT security controls.

**Scope of this description:** This section is not intended to be a complete description of all Physical Asset Management domains. This section focuses on the key Physical Asset Management components that contribute to security.

Figure 2-10 shows an overview of the Physical Asset Management subcomponents and the related components from the Security Services and Infrastructure layer.

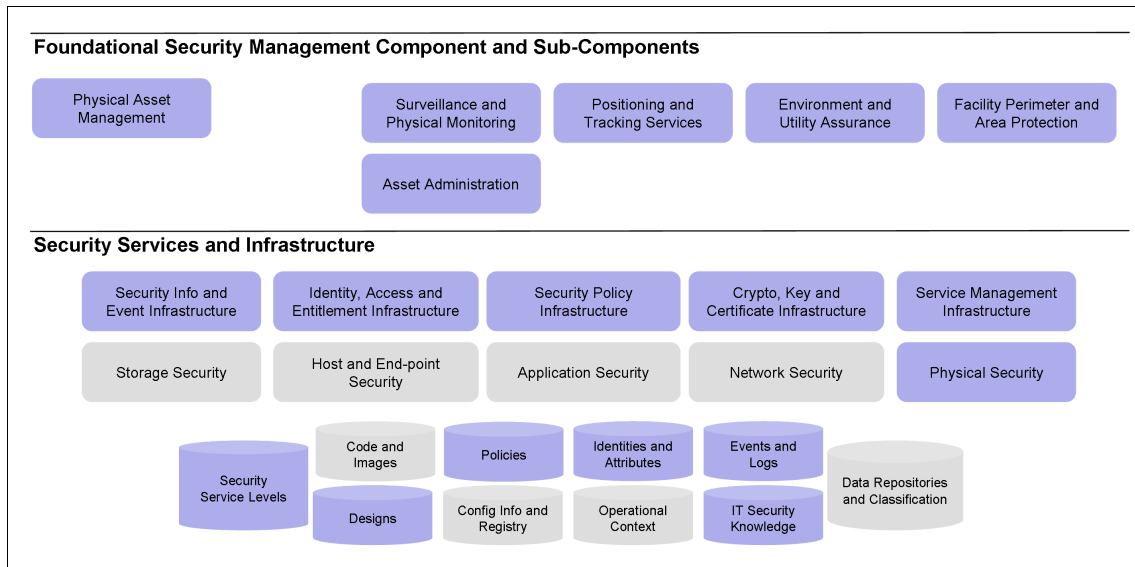


Figure 2-10 Physical Asset Management subcomponents

Because of the ongoing convergence of physical and IT security, Physical Asset Management is a major concern, although it builds its own discipline in IT management and has a much wider purpose.

Physical Asset Management consists of the following subcomponents:

- ▶ Surveillance and Physical Monitoring
- ▶ Environment and Utility Assurance
- ▶ Facility, Perimeter, and Area Protection
- ▶ Positioning and Tracking Services
- ▶ Asset Administration

These subcomponents are explained in the following sections.

## **Surveillance and Physical Monitoring**

Surveillance and Physical Monitoring covers all investigative physical security controls and is the equivalent of IT technical monitoring, including real-time observation of physical assets to detect physical attacks, theft, abuse, and other unusual and suspicious events. Such controls can include physical alarm systems that are triggered by opening doors and gates, breaking or opening windows and hatches, moving objects, or simple discovery of intruders because of motion detection. Surveillance and Physical Monitoring can be performed by using direct or indirect human supervision or automated systems that can analyze changes in normal and infrared light or sound patterns of the monitored area. Surveillance and Physical Monitoring can record evidence over a longer period to investigate security-related situations retrospectively.

## **Environment and Utility Assurance**

Environment and Utility Assurance covers the provisioning of electricity and other utility-related supplies and climate controls, which also includes water and gas monitoring systems that supply the facility. Environment and Utility Assurance is a part of facility management that can have a significant impact on the availability of IT services and hence on security.

## **Facility, Perimeter, and Area Protection**

Facilities, Perimeter, and Area Protection covers the provisioning and management of preventive, deterrent, and reactive physical security and safety controls of a human or automatic nature. This service includes site-planning activities to address known risks from natural disaster, political events, and other external threats. Fire suppression and monitoring systems are also included in this service.

## **Positioning and Tracking Services**

Positioning and Tracking Services are related to the identification of the location and movement of tangible physical assets, in this context, of those assets with valuable information that must be protected. This component can include short-range and long-range tracking, up to a worldwide scale.

## **Asset Administration**

Asset Administration covers the coordination of activities that are related to the provisioning, building and procurement, maintenance and updating, movement, decommissioning, and destruction of primarily tangible but also non-tangible physical assets. These activities go beyond pure IT assets, but mostly focus on assets that have a direct or significant impact on information security. Examples of such assets include, but are not limited to, real estate buildings that provide office floor space or data centers, cable and utility channels, and data tape storage containers and their transportation vehicles.

## Security Services and Infrastructure components

The following Security Services and Infrastructure components are key to effective Physical Asset Management (depicted as blue-shaded objects in Figure 2-10 on page 101):

- ▶ **Security Information and Event Infrastructure**

The information about physical environments that are recorded through surveillance and sensors is increasingly being indexed and converted to IT security events that can be correlated and combined with other IT events. For example, an authorization record about the access of an application can be correlated with an event that represents a person using their badge to access a door. Likewise, these records can be correlated with segments of video surveillance footage with matching timestamps.

- ▶ **Identity, Access, and Entitlement Infrastructure**

High-value assets in a physical environment are often protected by both physical controls (fences, guards, and so on) and logical access (badge readers and RFID detectors).

- ▶ **Security Policy Infrastructure**

The Security Policy Infrastructure that is used to manage organization roles and their entitlements to IT resources, such as applications, can also be used to manage the policies that govern activities in the physical environment. For example, the Security Policy Infrastructure can be used to author the policies that security personnel use to enforce access control if a person can or cannot pass a physical checkpoint on the premises.

- ▶ **Cryptography, Key, and Certificate Infrastructure**

Many physical credentials, such as access badges, smart cards, or passports, are increasingly embedding logical credentials, such as public key certificates, which must be managed by a Cryptography, Key, and Certificate Infrastructure.

- ▶ **Service Management Infrastructure**

Service Management Infrastructure processes are often combined to manage both IT security and physical security incidents so that one service desk and one workflow infrastructure can manage both in one place.

- ▶ **Physical Security**

The Physical Security infrastructure, including barriers, fences, secure construction, and other types of inert security, can provide a base for providing an overall secure environment for an organization. The personnel, such as security guards and inspectors, add to the base security by enforcing operational processes on a day-to-day basis.

The runtime aspects of Physical Security depend on the Physical Security infrastructure. For example, the placement of surveillance equipment depends on the layout of the physical environment. If the physical environment is not designed with security in mind, it can be more difficult to place surveillance equipment effectively.

- ▶ **Security Service Levels**

The security service level agreements must, at least, delegate authority for Physical Security to an accountable person. Certain agreements even define fine-grained details, such as specific physical controls (barriers and perimeter checkpoints).

- ▶ **Designs**

The designs of the physical layout of an organization's perimeter can have a large impact on the required surveillance and sensors that must be in place. A good design includes Physical Asset Management requirements from the beginning.

- ▶ **Policies**

Policies that are related to the Physical Security of assets can depend on an organizational directory and organizational roles in the same way that access policies for securing IT resources do. Likewise, policies for securing physical assets are a necessary component to the overall IT security and should be included in the library of all security policies and be subject to the same review and change processes.

- ▶ **Identities and Attributes**

Physical asset security depends on directories of employees and their organizational roles to control access to physical assets and to manage who can use or maintain the high-value physical assets. For example, a Physical Security policy might require that only people who have completed a particular training program should be allowed to perform maintenance on a physical asset.

## **2.3 Conclusion**

This chapter explained the IBM Security Blueprint in more detail by describing the components and subcomponents of the IBM Security Blueprint. This chapter described the subcomponents in detail and related them to the key infrastructure and security services components on which they depend.

The next chapter provides an overview of well-known industry frameworks and standards to put the IBM Security Framework and IBM Security Blueprint into perspective.





# IT security frameworks and standards

Today, you have access to various industry frameworks, standards, and guidance that can help you design IT enterprise security. This chapter provides an overview of some of the most common of them and looks at their relationship with the IBM Security Blueprint and IBM Security Framework.

Driven by business reasons, more organizations today are looking to adopt internationally accepted frameworks and preferred practices to help implement IT governance for their operations. Also, to comply with external regulations, different sets of preferred practices were developed over the past years.

The goal of this chapter is to provide an overview of the underlying structure and principles of the inter-relationships within organizations. We want to show you how to integrate and align industry information security and privacy standards-based frameworks with the IBM Security Blueprint.

This chapter includes the following sections:

- ▶ Industry information security and privacy standards profile model
- ▶ TOGAF
- ▶ IBM Unified Method Framework
- ▶ Sherwood Applied Business Security Architecture
- ▶ Control Objectives for Information and Related Technology
- ▶ ISO/IEC 27002:2005

- ▶ Payment Card Industry Data Security Standard
- ▶ Sarbanes-Oxley Act
- ▶ Health Insurance Portability and Accountability Act

### 3.1 Industry information security and privacy standards profile model

Working in the area of information security requires a broad range of understanding when it comes to information technology and its integration into a business environment. The increasing number of externally imposed and controlled regulations and standards does not make this task any easier. Most of these regulatory measurements are defined for particular industry sectors.

To design IT security solutions, or any other IT solution, for an organization, IT architects like to rely on well-known and established frameworks. Aligning your work with any of those frameworks provides several benefits, including a step-by-step approach, verification or even certification of results, a holistic viewpoint, and others. Most of these frameworks can be applied in a cross-industry manner.

In our information security and privacy standards profile model, which is shown in Table 3-1, we want to provide you with an overview of some of the more common standards and frameworks. This model is far from exhaustive. The Government column, for example, can potentially be extended with regulatory guidelines for many countries around the world; all these standards are in a continuous evolution. Even the standards in the other columns experience constant change.

Table 3-1 Information security and privacy standards profile model

Financial	Government	Healthcare	Media and Entertainment	Cross industry
Payment Card Industry Data Security Standard (PCI DSS)	Advertising Standards Authority (ASA)	Health Insurance Portability and Accountability Act (HIPAA)	Personal Information Protection and Electronics Document Act (PIPEDA)	Control Objectives for Information and Related Technologies (COBIT)
Gramm - Leach - Bliley Act (GLBA)	The Department of Defense Architecture Framework (DoDAF)	HITRUST Common Security Framework (CSF)		International Organization for Standardization (ISO 27002:20XX)

Financial	Government	Healthcare	Media and Entertainment	Cross industry
Federal Information Processing Standard (FIPS)	Family Educational Rights and Privacy Act (FERPA)			Open Group Architecture Framework (TOGAF)
Bank for International Settlements (Basel III)	National Institute of Standards and Technology (NIST)			Information Technology Infrastructure Library (ITIL)
Sarbanes - Oxley Act (SOX)				IBM Unified Method Framework (UMF)
Financial Sector Implementation Assistance (FISAP)				Open Enterprise Security Architecture (O-ESA)
European Union Data Protection Directive (EUDPD)				Sherwood Applied Business Security Architecture Framework (SABSA)
				Trusted Cloud Initiative Reference Architecture (TCI)

In the remainder of this chapter, we take more time to investigate several of the more common frameworks and regulatory standards. We picked five frameworks that have a great significance for many organizations around the globe.

- ▶ TOGAF
- ▶ IBM UMF
- ▶ SABSA
- ▶ COBIT
- ▶ ISO 27002

As a practical example about how the IBM Security Blueprint can be used in combination with another framework, Chapter 4, “Using O-ESA to develop an enterprise security architecture” on page 145 covers one architecture framework in more detail.

In addition to these architecture frameworks, this chapter also examines three regulatory standards because they have an important worldwide impact.

- ▶ PCI-DSS
- ▶ SOX
- ▶ HIPAA

## 3.2 TOGAF

TOGAF, an Open Group Standard, is an architecture framework that provides methods and tools for assisting you with the acceptance, production, usage, and maintenance of an enterprise architecture. TOGAF is based on an iterative process model that is supported by preferred practices and a reusable set of existing architecture assets. TOGAF helps practitioners avoid being locked into proprietary methods, use resources more efficiently and effectively, and realize a greater return on investment (ROI). First developed in 1995, TOGAF was based on the US Department of Defense Technical Architecture Framework for Information Management (TAFIM). The Open Group Architecture Forum developed successive versions of TOGAF at regular intervals and published them on The Open Group public website at:

<http://www.opengroup.org>

The latest release of TOGAF, at the time of writing this book, is Version 9.1. For the remainder of this chapter, we simply refer to it as TOGAF.

Let us now take a closer look at TOGAF in the following sections:

- ▶ What is architecture in the context of TOGAF
- ▶ Industry guidance and techniques
- ▶ IBM Security Blueprint mapping

### 3.2.1 What is architecture in the context of TOGAF

ISO/IEC 42010: 2007<sup>1</sup> defines *architecture* as “the fundamental organization of a system, embodied in its components, their relationships to each other and the environment, and the principles governing its design and evolution.”

---

<sup>1</sup> The full definition can be found at  
<http://www.iso-architecture.org/ieee-1471/defining-architecture.html>.

TOGAF embraces but does not strictly adhere to ISO/IEC 42010: 2007 terminology. In TOGAF, architecture has two meanings, depending upon the context:

- ▶ A formal description of a system, or a detailed plan of the system at the component level to guide its implementation.
- ▶ The structure of components, their inter-relationships, and the principles and guidelines that govern their design and evolution over time.

TOGAF considers the enterprise as a system and tries to strike a balance between promoting the concepts and terminology of ISO/IEC 42010: 2007 and ensuring that the usage of terms that are defined by ISO/IEC 42010: 2007 is consistent with the standard and retaining other commonly accepted terminology that is familiar to most of the TOGAF readership.

Table 3-2 provides an overview of the TOGAF structure.

*Table 3-2 TOGAF structure overview*

TOGAF Part	Overall Description
Part I: Introduction	This part provides a high-level introduction to the key concepts of enterprise architecture and, in particular, to the TOGAF approach. It contains the definitions of terms that are used throughout TOGAF.
Part II: Architecture Development Method	This part defines the core of TOGAF. It describes the TOGAF Architecture Development Method (ADM), which is a step-by-step approach to developing an enterprise architecture.
Part III: ADM Guidelines and Techniques	This part contains a collection of guidelines and techniques that are available for use in applying the ADM.
Part IV: Architecture Content Framework	This part describes the TOGAF content framework, including a structured metamodel for architectural artifacts, the use of reusable Architecture Building Blocks (ABBs), and an overview of typical architecture deliverables.
Part V: Enterprise Continuum and Tools	This part describes the appropriate taxonomies and tools to categorize and store the outputs of architecture activity within an enterprise.

TOGAF Part	Overall Description
Part VI: TOGAF Reference Model	This part provides two architectural reference models, namely the TOGAF Technical Reference Model (TRM), and the Integrated Information Infrastructure Reference Model (III-RM).
Part VII: Architecture Capability Framework	This part describes the organization, processes, skills, roles, and responsibilities that are required to establish and operate an architecture practice within an enterprise.

### 3.2.2 Architecture types that are supported by TOGAF

TOGAF covers the development of four related types of architecture, which is shown in Table 3-3. These four types of architecture are commonly accepted as subsets of an overall enterprise architecture, all of which TOGAF is designed to support.

Table 3-3 TOGAF architecture types

Architecture type	Overall description
Business Architecture	The business strategy, governance, organization, and key business processes.
Data Architecture	The structure of an organization's logical and physical data assets and data management resources.
Application Architecture	A blueprint for the individual applications to be deployed, their interactions, and their relationships to the core business processes of the organization.
Technology Architecture	The logical software and hardware capabilities that are required to support the deployment of business, data, and application services. These capabilities include IT infrastructure, middleware, networks, communications, processing, and standards.

### 3.2.3 Industry guidance and techniques

This section takes a closer look at the following details:

- ▶ TOGAF content overview
- ▶ TOGAF Architecture Development Method (ADM)
- ▶ ADM guidelines and techniques

#### TOGAF content overview

TOGAF includes the concept of the Enterprise Continuum, which is shown in Figure 3-1.

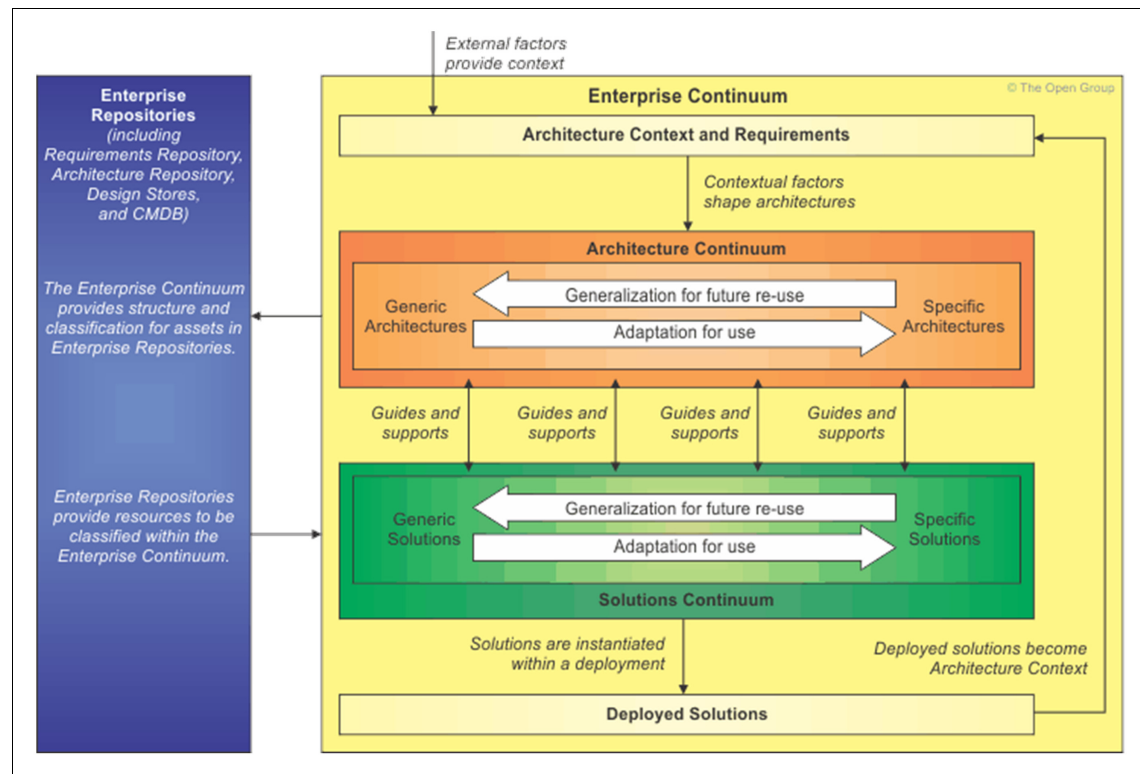


Figure 3-1 TOGAF Enterprise Continuum

The concept defines the broader context for an architect and explains how generic solutions can be used and specialized to support the requirements of an individual organization. The Enterprise Continuum is a view of the Architecture Repository that provides methods for classifying architecture and solution artifacts as they evolve from generic *foundation architectures* to *organization-specific architectures*. The Enterprise Continuum is composed of two complementary concepts: the Architecture Continuum and the Solutions Continuum.

### **TOGAF Architecture Development Method (ADM)**

The TOGAF Architecture Development Method (ADM) is a generic method for developing and managing the lifecycle of an enterprise architecture, and forms the core of TOGAF. It integrates elements of TOGAF and other available architectural assets to meet the business and IT needs of an organization.

The ADM provides a tested and repeatable process for developing architectures. The ADM helps you establish an architecture framework, develop architecture content, and migrate and govern the realization of architectures. All of these activities are carried out within an iterative cycle of continuous architecture definition and realization that allows organizations to transfer their enterprises in a controlled manner in response to business goals and opportunities.



The phases within the TOGAF ADM are shown in Figure 3-2.



Figure 3-2 TOGAF Architecture Development Method (ADM)

Here we examine the phases within the ADM in more detail:

► Preliminary Phase

This phase describes the preparation and initiation activities that are required to create an architecture capability, including the customization of TOGAF and definition of architecture principles.

- ▶ **Phase A: Architecture Vision**  
This phase describes the initial phase of an architecture development cycle. It includes information about defining the scope of the architecture development initiative, identifying the stakeholders, creating the architecture vision, and obtaining approval to proceed with the architecture development.
- ▶ **Phase B: Business Architecture**  
This phase describes the development of a business architecture to support the agreed architecture vision.
- ▶ **Phase C: Information Systems Architectures**  
This phase describes the development of information systems architectures to support the agreed architecture vision.
- ▶ **Phase D: Technology Architecture**  
This phase describes the development of the technology architecture to support the agreed architecture vision.
- ▶ **Phase E: Opportunities & Solutions**  
This phase conducts initial implementation planning and the identification of delivery vehicles for the architecture that is defined in the previous phases.
- ▶ **Phase F: Migration Planning**  
This phase addresses how to move from the baseline to the target architectures by finalizing a detailed implementation and migration plan.
- ▶ **Phase G: Implementation Governance**  
This phase provides an architectural oversight of the implementation.
- ▶ **Phase H: Architecture Change Management**  
This phase establishes procedures for managing change to the new architecture.
- ▶ **Requirements Management**  
This phase examines the process of managing architecture requirements throughout the ADM.

### **ADM guidelines and techniques**

ADM guidelines and techniques support the application of the ADM. The guidelines address adapting the ADM to deal with many use cases, including different process styles (for example, the use of iteration) and also specific specialty architectures, such as security. The techniques support specific tasks within the ADM (such as defining principles, business scenarios, gap analysis, migration planning, and risk management).

### 3.2.4 IBM Security Blueprint mapping

The IBM Security Blueprint can play a role during the first phases of the TOGAF Architecture Development Method, and it can also be used to create some of the architectural artifacts. Let us examine a few examples:

- ▶ Presume that the IBM Security Blueprint can be reused through phases A to D of the TOGAF ADM. In phase A, it can help you define a security strategy and vision through the selection of security capabilities that should be provided. In phase B, the security services catalog can be built around the subcomponents of the IBM Security Blueprint. In Phase C, the capabilities from the Data and Information Protection Management component can be used, and finally in phase D, the Infrastructure Foundational Security Management component can describe the building blocks in that layer.
- ▶ The subcomponents of the IBM Security Blueprint with their capabilities can serve as Architecture Building Blocks at several levels of the TOGAF Content Metamodel. For example, as part of the Business Architecture, the necessary security services can be built around subcomponents of the IBM Security Blueprint.
- ▶ The taxonomy that is provided by the IBM Security Blueprint can be reused, and possibly adapted, in the architecture repository. As part of the Architecture Continuum, the IBM Security Blueprint can be further used as a foundation to develop more specific solution descriptions (realization at the infrastructure layer) as part of the Solution Continuum in the Architecture Repository.
- ▶ The subcomponents of the IBM Security Blueprint can provide defined security services that are built around their capabilities. These services are part of the Security Category in the Technical Reference Model (TRM) of TOGAF.
- ▶ This usage is applicable both for generic enterprise architecture and an Enterprise Security Architecture developed through the ADM cycles.

## 3.3 IBM Unified Method Framework

The IBM Unified Method Framework (UMF) is an evolution of the IBM Global Services Method. UMF provides a common language among all practitioners that deliver business solutions, and it is being used as a fundamental component of asset-based services that deliver the basic building blocks and mechanisms for practitioners to reuse knowledge and assets that are based on a consistent and integrated approach.

The UMF is an extensible integration framework that defines a *common language* for the interoperation of practices. A *practice* is a component of a process that can be adopted by an organization to build an organizational capability.

The UMF Method Framework, which is depicted in Figure 3-3, represents a consistent and repeatable approach to accomplish a set of objectives that are based on a collection of well-defined techniques and preferred practices. The Method Framework consists of Method Content and Processes.

- ▶ Method Content represents the primary reusable building blocks of the method that exist outside of any predefined lifecycle.
- ▶ A Process is used to assemble Method Content into a sequence or workflow that is represented by a work breakdown structure, which is used to organize the project and develop architecting solutions.

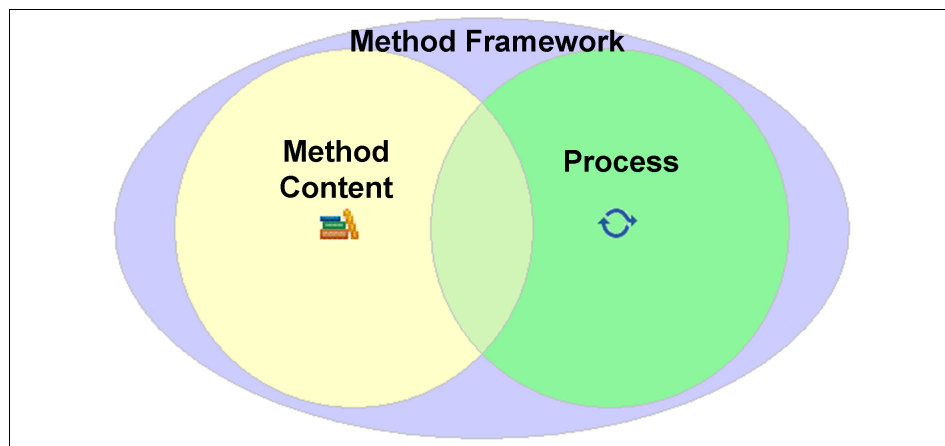


Figure 3-3 IBM Unified Method Framework

### 3.3.1 Industry guidance and techniques

The Unified Method Framework defines method architecture, standardized categorization schemes and views, and method authoring guidance to simplify method development and enable development and sharing of method assets across organizations and teams. Central to the UMF is the concept of *practices*. Practices represent a documented approach to solving one or more commonly occurring problems. Practices are loosely coupled, so they can be independently adopted to support incrementally measured improvement initiatives. Each practice includes guidance about when and how to adopt the practice, guidance about how to perform the practice by using IBM Rational® tools, and guidance about recommended measurements and metrics to assess practice adoption, project or product status, and compliance to common standards.

The UMF establishes a single framework library and common standards for integration. The overall integration model is depicted in Figure 3-4.

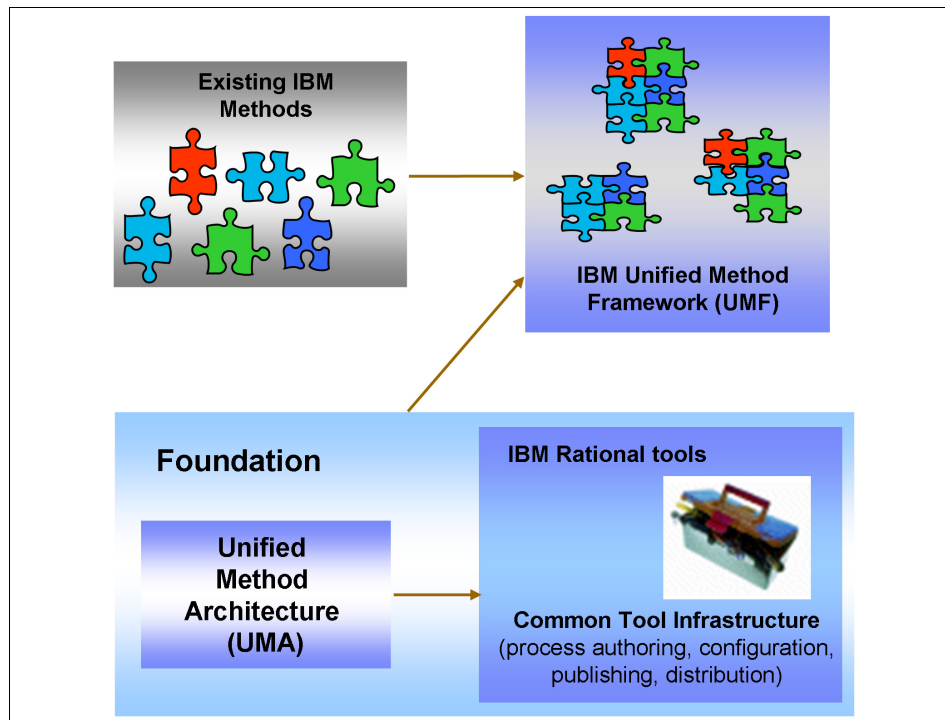


Figure 3-4 UMF integration model

The UMF provides the following consistent constructs at a global level:

- Vocabulary
- Output
- Input
- Deliverables
- Roles
- Guidance
- Work products or artifacts
- Processes

The method is used to reduce or avoid a misunderstanding of terms, insecurity about the approach to the business solution, and confusion about work products or artifacts and deliverables to be created.

### UMF domain

The UMF *domain* is the primary way work products or artifacts are organized. UMF *subdomains* are used to further organize work products into more fine-grained artifacts. This structure is shown in Figure 3-5.

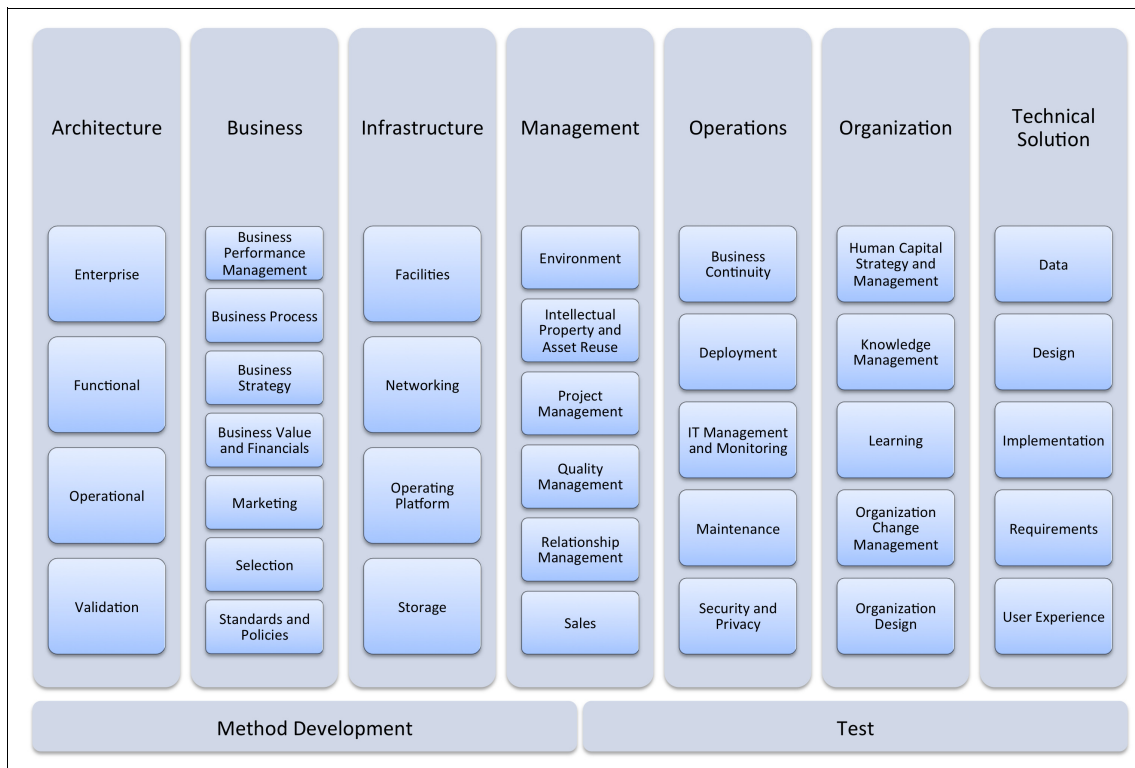


Figure 3-5 UMF domain model

A domain is not specific to a particular type of development environment, for example, system development, hardware development, or software development. Domains do not tend to fluctuate much; no changes are required when a new type of development is identified.

Work products that are categorized to top-level domains typically apply across all or most subdomains; top-level domains should not be considered a container for work products that do not fit in one of the subdomains.

A domain describes an area of the method to be governed and maintained by a particular authoring group to ensure consistency and minimize overlap. A domain guides the general usage for all work products that are mapped to that domain.

Domains do not restrict the usage of work products or artifacts that are mapped to that domain. For example, if a work product is primarily business-oriented, then the Business domain is the best place to look; however, that does not mean work product cannot cover other concepts.

### **UMF delivery process**

The UMF delivery processes and practices are associated with a delivery process through their assigned publishing contexts. Publishing contexts are the main way of grouping content for publishing.

A publishing context may include one or more delivery processes or practices.

There are five process families for practices:

- ▶ Business Practices
- ▶ General Practices
- ▶ Management Practices
- ▶ Operations Practices
- ▶ Technical Practices

### **3.3.2 IBM Security Blueprint mapping**

The IBM Security Blueprint can provide a good foundation for some of the UMF artifacts. For example, for the Architecture domain, the IBM Security Blueprint can provide standard components to a functional model for a security solution. You can use the foundational security management components and their corresponding subcomponents to describe a security component model. Also, the taxonomy of the IBM Security Blueprint can help define organizational standards and policies (by using the UMF artifacts in the business domain).

## 3.4 Sherwood Applied Business Security Architecture

The Sherwood Applied Business Security Architecture Framework<sup>2</sup> (SABSA) is a methodology for developing risk-driven enterprise information security and information assurance architectures and for delivering security infrastructure solutions that support critical business. SABSA is used successfully by numerous organizations around the world.

SABSA can help ensure that the needs of your organization are met and that security services are designed, delivered, and supported as a part of your business and IT management infrastructure.

Although copyright protected, SABSA is an *open-use methodology*, not a commercial product.

SABSA is a six layer model for a security architecture that is widely accepted today. The starting point for this work was ISO 7498-2 1989 (Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture). This standard is relatively unsophisticated in terms of business drivers, but it defines an important framework in terms of security services, logical architecture and security mechanisms, physical architecture and security management, and operational architecture. The Sherwood team added two upper layers to provide a business-driven approach (contextual and conceptual architectures), and a lower layer to map onto real tools and products (component architecture).

Unknown to Sherwood at the time, this work was closely related to work being carried out in the US on the wider context of overall enterprise architectures. This work was authored by John Zachman, which is published by the Zachman Institute for Framework Advancement, and known as the *Zachman Framework*.<sup>3</sup>

---

<sup>2</sup> More information about SABSA can be found at <http://www.sabsa-institute.org>.

<sup>3</sup> More information about the Zachman Framework can be found at <http://www.zachmaninternational.com/index.php/the-zachman-framework>.



### 3.4.1 Common strategy and terminology

Common strategy and terminology must be tightly business-oriented to maintain a common understanding across all potentially used security frameworks and methods. The primary business requirements for information security are business-specific. These requirements are expressed in terms of protecting the availability, integrity, authenticity, and confidentiality of business information, and providing accountability and auditability for IT systems. To understand these requirements, a detailed analysis of the business processes is required, using as source data information gathered by interviews with operational business managers. The generic business requirements for an information security solution often include the following items:

- ▶ Low-cost development  
Is the solution of modular design and hence capable of being integrated into a development program at minimal cost?
- ▶ Fast time to market  
Is the solution capable of being integrated into a development program with minimal delay to meet the time frames that are associated with windows of business opportunity?
- ▶ Scalability of cost  
Is the entry-level cost appropriate to the range of business applications for which the solution is intended?
- ▶ Scalability of platforms  
Does the solution fit with the range of computing platforms with which it might be required to integrate?
- ▶ Scalability of security level  
Does the solution support the range of cryptographic and other techniques that are needed to implement the required range of security strengths and assurance levels?
- ▶ Scalability of use  
Is the solution capable of being scaled to meet future numbers of business users or future capacity requirements for throughput and storage of information and transaction volumes?
- ▶ Reusability  
Is the solution reusable in various similar situations to get the best ROI in its acquisition and development?
- ▶ Operations costs  
Can the cost impact on systems operations be minimized?

- ▶ Administration costs

Does the solution provide an efficient means for security administration to minimize the costs of this activity?
- ▶ Usability

Is the solution appropriate to the technical competence of the intended users and will it be ergonomically acceptable to those users?
- ▶ Inter-operability

Does the solution provide for the long-term requirements for inter-operability between communicating IT systems and applications?
- ▶ Integration

Does the solution integrate with the wide range of computer applications and platforms for which it might be required in the long term?
- ▶ Supportability

Is the solution capable of being supported in the environment within which it is designed to be used?
- ▶ Risk-based cost and benefit effectiveness

Is the reduction of risk (the benefit) appropriate to the costs of acquisition, development, installation, administration, and operation?
- ▶ Enabling business

Finally, there are many business-specific requirements that influence the security strategy, which include requirements where security has an important role in generating the appropriate level of confidence to enable new ways of doing business using the latest advances in information technology.

### **3.4.2 Industry guidance and techniques**

This section looks in to the following aspects:

- ▶ SABSA model
- ▶ SABSA matrix

## SABSA model

SABSA is a methodology for developing risk-driven enterprise information security and information assurance architectures and for delivering security infrastructure solutions that support critical business initiatives. The SABSA methodology is defined in the *SABSA model*, a top-down approach that drives the SABSA Development Process. This process analyzes the business requirements at the outset, and creates a chain of traceability through the SABSA lifecycle phases of Strategy & Planning, Design, Implement, and ongoing Manage & Measure to ensure that the business mandate is preserved. SABSA methodology is described in the SABSA Blue Book, *Enterprise Security Architecture: A Business-Driven Approach*, by Sherwood, et al.

The SABSA model is composed of six layers, the summary of which is depicted in Figure 3-6. Each layer represents the view of a different player while specifying, designing, constructing, and using the business system.

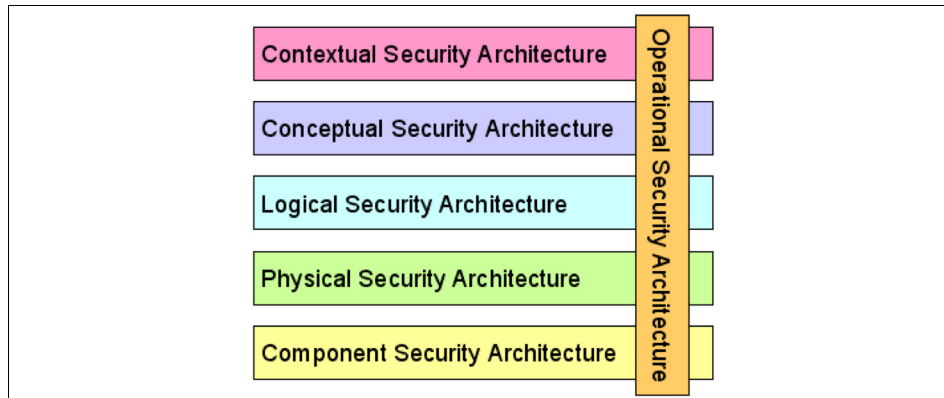


Figure 3-6 SABSA model for security architecture

For a detailed analysis of each of the six layers, the SABSA Matrix also uses the same six questions that are used in the Zachman Framework:

- ▶ *What* are you trying to do at this layer?  
What are the assets to be protected by your security architecture?
- ▶ *Why* are you doing it?  
What is the motivation for wanting to apply security, expressed in the terms of this layer?
- ▶ *How* are you trying to do it?  
What functions are needed to achieve security at this layer?

- ▶ *Who* is involved?

Who are the people and what are the organizational aspects of security at this layer?

- ▶ *Where* are you doing it?

What are the locations where you apply your security, relevant to this layer?

- ▶ *When* are you doing it?

What are the time-related aspects of security that are relevant to this layer?

## SABSA matrix

These six vertical architectural elements are now summarized for all six horizontal layers, which produces a 6 x 6 matrix of cells that represents the whole model for the enterprise security architecture. It is called the SABSA matrix (see Figure 3-7). If you can address the issues that are raised by each of these cells, then you have covered the entire range of questions to be answered, and you can have a high level of confidence that your security architecture is complete.

SABSA MASTER MATRIX						
	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECTURE	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
	Taxonomy of Business Assets, including Goals & Objectives	Opportunities & Threats Inventory	Inventory of Operational Processes	Organisational Structure & the Extended Enterprise	Inventory of Buildings, Sites, Territories, Jurisdictions, etc.	Time dependencies of business objectives
CONCEPTUAL ARCHITECTURE	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain Framework	Time Management Framework
	Business Attributes Profile	Enablement & Control Objectives; Policy Architecture	Process Mapping Framework; Architectural Strategies for ICT	Owners, Custodians and Users; Service Providers & Customers	Security Domain Concepts & Framework	Through-Life Risk Management Framework
LOGICAL ARCHITECTURE	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Framework	Domain Maps	Calendar & Timetable
	Inventory of Information Assets	Domain Policies	Information Flows; Functional Transformations; Service Oriented Architecture	Entity Schema; Trust Models; Privilege Profiles	Domain Definitions; Inter-domain associations & interactions	Start Times, Lifetimes & Deadlines
PHYSICAL ARCHITECTURE	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	ICT Infrastructure	Processing Schedule
	Data Dictionary & Data Inventory	Risk Management Rules & Procedures	Applications; Middleware; Systems; Security Mechanisms	User Interface to ICT Systems; Access Control Systems	Host Platforms, Layout & Networks	Timing & Sequencing of Processes and Sessions
COMPONENT ARCHITECTURE	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Management Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools
	ICT Products, including Data Repositories and Processors	Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools	Tools and Protocols for Process Delivery	Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists	Nodes, Addresses and other Locators	Time Schedules; Clocks, Timers & Interrupts
SERVICE MANAGEMENT ARCHITECTURE	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time & Performance Management
	Assurance of Operational Continuity & Excellence	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Applications & Services	Account Provisioning; User Support Management	Management of Buildings, Sites, Platforms & Networks	Management of Calendar and Timetable

Figure 3-7 SABSA matrix

The generic structure of both SABSA and The Open Group TOGAF enterprise architecture methodology are built on similar principles as the John Zachman Framework (see the six questions that characterize the Zachman Framework that is used in SABSA, and the known fact that TOGAF populates the Zachman Framework).

### 3.4.3 IBM Security Blueprint mapping

When you look at the SABSA model in general, and more specifically at the SABSA matrix in Figure 3-7 on page 125, you can see the possible usage of the IBM Security Blueprint at the three upper layers of the SABSA model (conceptual, contextual, and logical architecture). As described in Chapter 7, “Using This Book as a Practical Guide”, of *Enterprise Security Architecture: A Business-Driven Approach*, by Sherwood, et al, several steps are needed to evolve from a business strategy towards a security strategy resulting in an operational model for the implementation of security controls.

The IBM Security Blueprint can be used to describe the logical security services as part of the *logical security architecture*. Answering the “how” question at this layer of the SABSA model can be addressed by a combination of capabilities by using the IBM Security Blueprint subcomponents and how they interact (the corresponding processes).

At this stage, SABSA defines *how the security services fit together as common reusable building blocks*, and this situation is where the IBM Security Blueprint can provide such building blocks in form of the foundational management components and subcomponents.

## 3.5 Control Objectives for Information and Related Technology

COBIT<sup>4</sup> is a framework that was created by the Information Systems, Audit, and Control Association (ISACA) and the IT Governance Institute (ITGI) in 1996. It is an internationally accepted framework that is based on defining the controls and processes that bridge the gap between the business and the Information Technology view of information security. The framework has gone through multiple releases over time. The latest version, Version 5, was published in 2012.

The previous release of COBIT, Version 4.1, released in 2007, focused on IT governance. The latest COBIT 5 framework integrates previous releases with ISACA’s *Risk IT* and *Val IT* frameworks to enhance the focus on *enterprise governance*.

Both Val IT and Risk IT are *principle-based* frameworks.

---

<sup>4</sup> Source: COBIT 5, 2012, © ISACA All rights reserved. Reprinted by permission. More information about COBIT can be found at <http://www.isaca.org/COBIT/Pages/default.aspx>.

## ***Risk IT***

Risk identification and mitigation are key aspects of an enterprise risk management discipline and enterprise governance in general. The Risk IT<sup>5</sup> framework focuses on IT-related risk areas for the business. It was released in 2009.

Risk IT is based on the principles that effective enterprise governance and management of IT risk provides the following aspects:

- ▶ Always connects to business objectives.
- ▶ Aligns the management of IT-related business risk with the overall enterprise risk management discipline.
- ▶ Balances the costs and benefits of managing IT risk.
- ▶ Promotes fair and open communication of IT risk.
- ▶ Establishes the right tone from the top while defining and enforcing personal accountability for operating within acceptable and well-defined tolerance levels.
- ▶ Is a continuous process and part of daily activities.

The Risk IT framework is structured as three domains:

- ▶ Risk Governance
- ▶ Risk Evaluation
- ▶ Risk Response

Each of these domains contains three processes that have objectives that are achieved by performing many activities.

## ***Val IT***

Business value delivery is another key aspect of enterprise governance. Val IT<sup>6</sup> is a framework that focuses on measuring business value of an organization's investments into information technology. It was released in 2008.

Here are the seven Val IT principles:

- ▶ IT-enabled investments are managed as a portfolio of investments.
- ▶ IT-enabled investments include the full scope of activities that are required to achieve business value.
- ▶ IT-enabled investments are managed through their full economic lifecycle.

---

<sup>5</sup> More information about Risk IT can be found at <http://www.isaca.org/Knowledge-Center/Risk-IT-IT-Risk-Management/Pages/Risk-IT-FAQ.aspx>

<sup>6</sup> More information about Val IT can be found at <http://www.isaca.org/Knowledge-Center/Val-IT-IT-Value-Delivery-/Pages/Val-IT-FAQ.aspx>.

- ▶ Value delivery practices recognize that there are different categories of investments that are evaluated and managed differently.
- ▶ Value delivery practices define and monitor key metrics and respond quickly to any changes or deviations.
- ▶ Value delivery practices engage all stakeholders and assign appropriate accountability for the delivery of capabilities and the realization of business benefits.
- ▶ Value delivery practices are continually monitored, evaluated, and improved.

The organization of the Val IT framework is structured according to three domains:

- ▶ Value Governance
- ▶ Portfolio Management
- ▶ Investment Management

Each of these domains contains many processes (22) that are each enabled by many key management practices (69).

Since its first release, COBIT has gone through several iterations and improvements that are depicted in Figure 3-8.

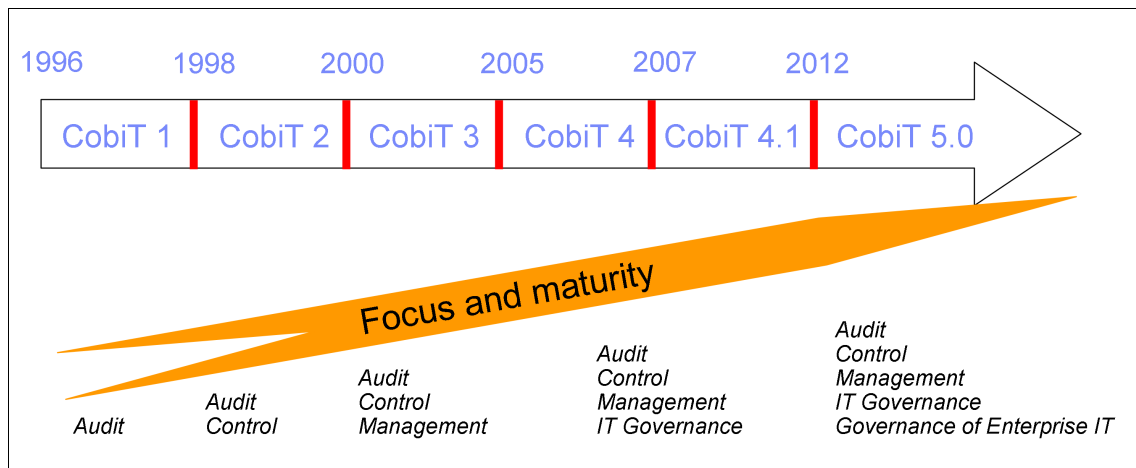


Figure 3-8 COBIT evolution

ISACA generally refreshes the COBIT framework about every three years. Every new release enhances the goals of previous releases and incorporates the latest trends in the IT industry.



### 3.5.1 COBIT 4.1

The previous edition of COBIT, Version 4.1, includes the following sections:

- ▶ Executive summary: Explains key concepts and principles.
- ▶ COBIT framework: Explains the general COBIT approach.
- ▶ Control objectives: Defines a generic set of control requirements that must be managed for each IT process to get effective control.
- ▶ Management guidelines: Explains tools to measure, compare, and improve the performance of IT processes.
- ▶ Implementation guide: Provides a tool set to implement COBIT.
- ▶ IT Assurance guide: Explains methods to assess whether control objectives are achieved.

The underlying concept of COBIT is that it looks at *business information* that every organization needs to support its business decisions. Business information itself is a result of IT-related resources, which COBIT defines as *applications, information, infrastructure, and people*. Finally, these IT-related resources are managed by IT processes to fulfill certain business information criteria (effectiveness, efficiency, confidentiality, integrity, availability, reliability, and compliance). This concept is presented in Figure 3-9.

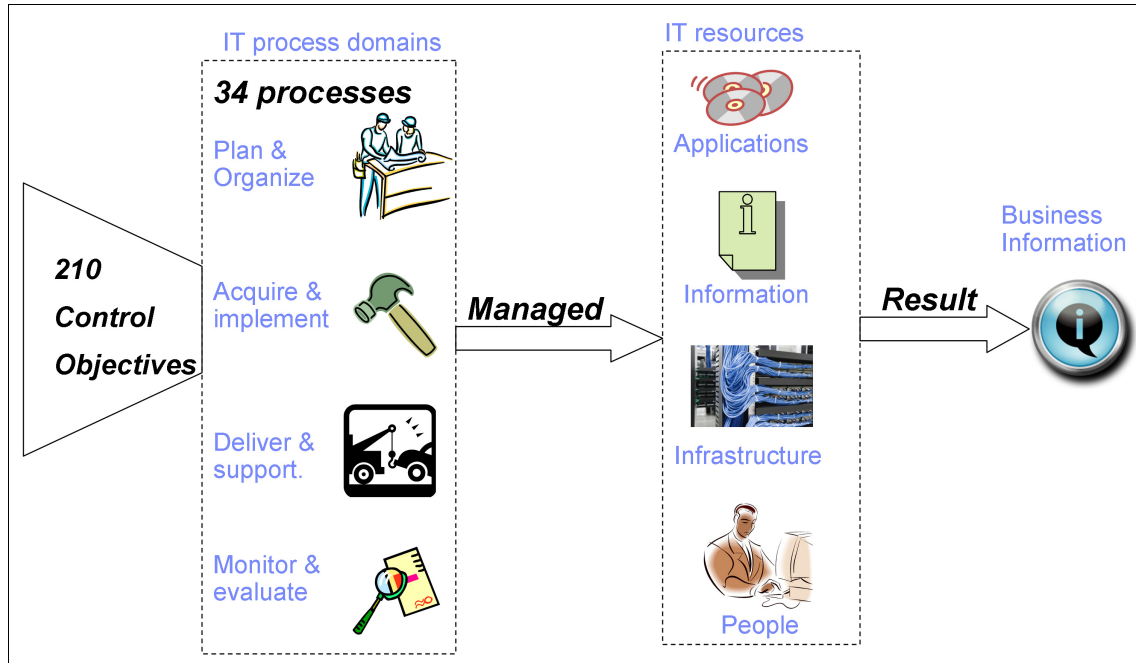


Figure 3-9 COBIT 4.1 concepts

COBIT 4.1 defines 34 high-level processes that are grouped into the following four domains:

- ▶ Plan and organize  
This domain focuses on IT strategy. How can IT contribute to business objectives?
- ▶ Acquire and implement  
The topic of this domain is the identification, development, or acquisition and integration of IT solutions to realize IT strategy.

- ▶ Deliver and support

This domain is about delivering and supporting the entire range of IT services.

- ▶ Monitor and evaluate

This domain focuses on the continuous assessment of all IT process to ensure their quality and compliance.

These 34 processes are controlled by 210 control objectives. Therefore, choose a top-down approach when you implement COBIT because business objectives must be clearly defined before the IT strategies can be aligned.

### **3.5.2 COBIT 5**

Although COBIT 4.1 was primarily focused on processes, COBIT 5 defines five principles that allow an organization to build an effective IT governance and management framework:

- ▶ Meeting stakeholder needs
- ▶ Covering the enterprise end-to-end
- ▶ Applying a single and integrated framework
- ▶ Enabling a holistic approach
- ▶ Separating governance from management

Another strong focus is on enablers. In COBIT 5, the following seven enablers (which are depicted in Figure 3-10) are defined:

- ▶ *Principles, policies, and frameworks* are the vehicle to translate the wanted behavior into practical guidance for day-to-day management.
- ▶ *Processes* describe an organized set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT-related goals.
- ▶ *Organizational structures* are the key decision-making entities in an enterprise.
- ▶ *Culture, ethics, and behavior* of individuals and of the enterprise are often underestimated as a success factor in governance and management activities.
- ▶ *Information* is required for keeping the organization running and well-governed, but at the operational level, information is often the key product of the enterprise itself.
- ▶ *Services, infrastructure, and applications* include the infrastructure, technology, and applications that provide the enterprise with information technology processing and services.
- ▶ *People, skills, and competencies* are required for successful completion of all activities, and for making correct decisions and taking corrective actions.

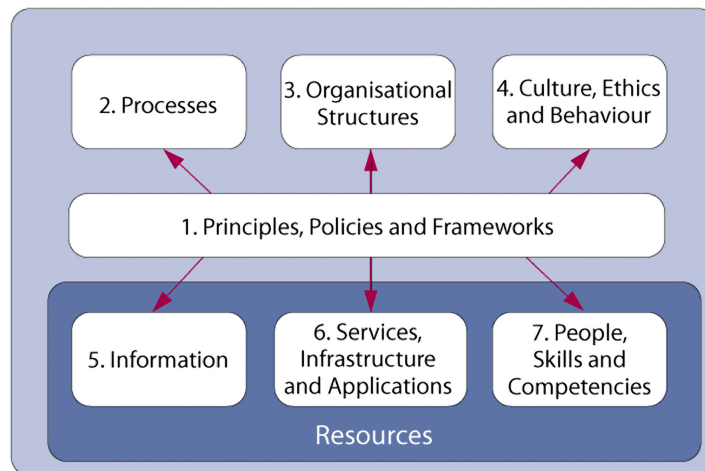


Figure 3-10 COBIT enablers

Although COBIT 4.1 used the concept of enablers, they were not so highlighted as in Version 5. As you can see in Figure 3-10 on page 132, a subset of COBIT 5 enablers were grouped as IT resources in COBIT 4.1. Processes were the central component for COBIT 4.1. Principles, policies, and frameworks were mentioned in some COBIT 4.1 processes, and culture, ethics, and behavior. Organizational structures were part of the role model in COBIT 4.1.

**More details:** A more detailed comparison between COBIT 4.1 and COBIT 5 can be found at:

<http://www.isaca.org/COBIT/Documents/COBIT5-Compare-With-4.1.ppt>

### 3.5.3 Maturity model and assessment using COBIT

Many organizations like to assess their IT security posture levels on a regular base. ISACA states that COBIT can be used as a reputable assessment method.

COBIT 4.1 and Risk IT and Val IT assessments are based on the COBIT Maturity Model (CMM) that defines the following six-level scale for posture assessment:

- ▶ Level 0: Non-existent
- ▶ Level 1: Initial/ad hoc
- ▶ Level 2: Repeatable but intuitive
- ▶ Level 3: Defined process
- ▶ Level 4: Managed and measurable
- ▶ Level 5: Optimized

The maturity models (MMs) in COBIT were first created in 2000. Then, they were designed based on the original CMM scale from the Carnegie Mellon Software Engineering Institute<sup>7</sup> (SEI) with the addition of an extra level 0.

COBIT 5 uses a different maturity model that is based on the ISO/IEC 15504 standard that is considered to be not compatible with the CMM approaches that are used in COBIT 4.1, Risk IT, and Val IT.

### 3.5.4 IBM capability mapping

By examining both the IBM Security Framework and the COBIT Framework, you can find many similarities in those approaches. The frameworks are both focused on bridging the gap between business and IT technical points of view with regard to security.

---

<sup>7</sup> For more information about the SEI Capability Maturity Model Integration, go to <http://www.sei.cmu.edu/cmmi/>.

The IBM Security Framework uses the COBIT model's approach to group IT resources for People, Information, Applications, and Infrastructure. It uses COBIT IT resources as the major security pillars to introduce a security view into the business realm. The IBM Security Framework also uses controls and a maturity model, which are concepts that are also a part of the COBIT Framework.

The IBM Security Blueprint provides a description of security capabilities that can be selected to fulfill the control objectives of COBIT.

### 3.6 ISO/IEC 27002:2005

The British Standard 7799 that preceded the International Organization for Standardization<sup>8</sup> 27002:2005 (ISO/IEC 27002:2005) is the most widely recognized security standard in the world. The standard started in 1992 as a Code of Practice that evolved into the British Standard 7799 in 1995. The last major publication was in May 1999, an edition that included many enhancements and improvements over previous versions. When it was republished in December 2000, it evolved into the International Organization for Standardization 17799 (ISO/IEC 17799). 17799 was republished again in 2005 as ISO/IES 17799:2005(E) with more revisions. In 2007, the name of ISO17799 was, without further amendment, adapted to the new ISO/IEC numbering scheme for information security management standards and is now identified as ISO/IEC 27002:2005.

ISO/IEC 27002:2005 is comprehensive in its coverage of security issues. It contains many control requirements, some of which are extremely complex. Compliance with ISO/IEC 27002:2005 is not a trivial task, even for the most security-conscious of organizations.

The development timeline of this standard is shown in Figure 3-11.

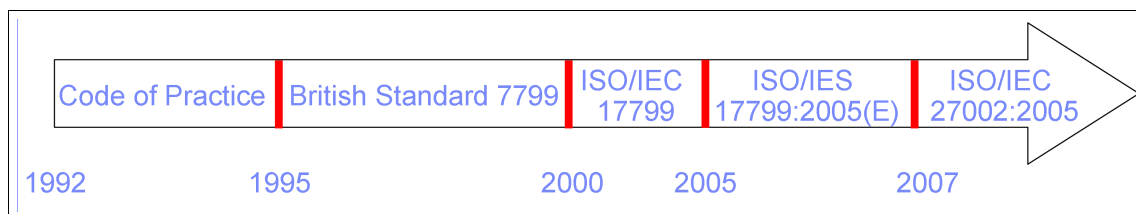


Figure 3-11 ISO/IEC 27002:2005 timeline

<sup>8</sup> Reprinted with the permission of ANSI on behalf of ISO. © ISO 2013 – All rights reserved. More information about the International Organization for Standardization can be found at <http://www.iso.org/iso/home.htm>.

A step-by-step manner of approaching ISO/IEC 27002:2005 is best. The best starting point is usually an assessment of the current position or situation, followed by an identification of the changes that are needed for ISO/IEC 27002:2005 compliance. From here, planning and implementing must be rigidly undertaken.

ISO/IEC 27002:2005 contains 12 categories, or domains, that must be considered when you apply an overall enterprise security approach. The categories are:

- ▶ Risk assessment
- ▶ Security policy
- ▶ Organization of information security
- ▶ Asset management
- ▶ Human resources security
- ▶ Physical and environmental security
- ▶ Communications and operations management
- ▶ Access control
- ▶ Information systems acquisition, development, and maintenance
- ▶ Information security incident management
- ▶ Business continuity management
- ▶ Compliance

Each of those 12 sections defines information security controls and their objectives relevant for the particular domain. The information security controls act as preferred practices or guidelines about how to achieve some objectives.

### **3.6.1 IBM Security Blueprint mapping**

The ISO 27002 standard provides guidance for the implementation of an Information Security Management System. It is exhaustive. Therefore, every organization that relies on this preferred practice should select the controls that are applicable for their information system or environment.

The foundational management components and subcomponents of the IBM Security Blueprint can be mapped to controls in one of the 11 categories of the ISO 27002. As such, the capabilities that are listed in the IBM Security Blueprint represent a subset of the required capabilities to realize all of the controls that are listed under the ISO 27002 standard.

The IBM Security Blueprint is meant to set a foundation for developing security architecture, although ISO 27002 provides the guidance to design an Information Security Management System (ISMS). Blueprints and architectures are means to describe and realize the goals that are defined in an ISMS.

## 3.7 Payment Card Industry Data Security Standard

The first credit card industry security standard, called the Cardholder Information Security Program (CISP), was originally developed and published by Visa in 2001. After you create their own individual data security standards, the major payment card brands decided to work together for the overall benefit of the payment card industry. Ultimately, Visa, MasterCard, American Express, Discover, and JCB became the primary founding members of the Payment Card Industry Security Standards Council (PCI SSC). They merged some of the best concepts of their own security standards to ultimately create a single, comprehensive payment industry-wide security standard that is known as the PCI Data Security Standard<sup>9</sup> (PCI DSS). The PCI DSS is a single cardholder data security standard that helps consolidate credit card processing security standards and associated compliance validation requirements.

### 3.7.1 IBM Security Blueprint mapping

Depending on the required type (merchant or service provider) and the implementation level, PCI provides the guidelines that must be followed to become PCI-compliant. The number of requirements that must be fulfilled depend on this type and level combination.

For most of the PCI control objectives, the IBM Security Blueprint describes the components and capabilities that can help fulfill those objectives. For example, the *Network Security* and *Host and Endpoint Security* capabilities of the *Software, System, and Service Assurance* foundational security management component can be used to satisfy PCI requirements for the *Build and Maintain a Secure Network* control objective. The IBM Security Blueprint defines many other relevant capabilities that can be used for the different PCI control objectives.

## 3.8 Sarbanes-Oxley Act

The Sarbanes-Oxley Act<sup>10</sup> (SOX) came into effect in July 2002 and introduced major changes to the regulation of corporate governance and financial practice. It is named after Senator Paul Sarbanes and Representative Michael Oxley, who were its main architects, and it set many non-negotiable deadlines for compliance.

---

<sup>9</sup> More information about PCS DSS can be found at <https://www.pcisecuritystandards.org>.

<sup>10</sup> More information about the Sarbanes-Oxley Act can be found at <http://www.soxlaw.com>.



The Sarbanes-Oxley Act is arranged into 11 *titles*. As far as compliance is concerned, the most important sections within these 11 titles are considered to be 302, 401, 404, 409, 802, and 906. Titles 302 and 404 are considered the most important from the IT governance and IT security perspective, as they relate to daily and annual financial reporting. As with many other frameworks, Sarbanes-Oxley focuses on the *what* and not the *how*. This kind of independence provides organizations with the choice of tools and methods for complying with the Sarbanes-Oxley Act.

### 3.8.1 Common strategy and terminology

Section 404 covers internal controls over financial reporting. Financial reporting covers the processes in place that are designed to ensure the reliability of the financial reporting process and the preparation of financial statements. This section mandates an annual evaluation of internal controls and procedures for company financial reporting. According to Section 302, the CEO and CFO must personally certify the evaluation of reports. The same section also requires the organization's external auditor to independently attest to management involvement on the effectiveness of internal controls, including IT controls, as they strongly relate to financial reporting.

SOX also has a strong impact on corporate governance and IT governance. Previously, internal control assertions were, usually, voluntary and based on varying guidelines, but this is no longer true. SOX does not specifically mention or refer to any specific security framework, but if you read SOX carefully, it is clear that the usage of any security framework is essential.

### 3.8.2 Industry guidance and techniques

This section describes at the following two subsections of SOX:

- ▶ Sarbanes-Oxley Act Section 302
- ▶ Sarbanes-Oxley Act Section 404

#### **Sarbanes-Oxley Act Section 302**

This section is listed under Title III of the act, and pertains to *Corporate Responsibility for Financial Reports*.

Periodic statutory financial reports are to include certifications that confirm the following information:

- ▶ The signing officers have reviewed the report.
- ▶ The report does not contain any material untrue statements or material omission or be considered misleading.

- ▶ The financial statements and related information fairly present the financial condition and the results in all material respects.
- ▶ The signing officers are responsible for internal controls and evaluated these internal controls within the previous 90 days and reported on their findings.
- ▶ A list of all deficiencies in the internal controls and information about any fraud that involves employees who are involved with internal activities.
- ▶ Any significant changes in internal controls or related factors that could have a negative impact on the internal controls.

Organizations may not attempt to avoid these requirements by reincorporating their activities or transferring their activities outside of the United States.

### **Sarbanes-Oxley Act Section 404**

This section is listed under Title IV of the act (Enhanced Financial Disclosures), and pertains to *Management Assessment of Internal Controls*.

Issuers are required to publish information in their annual reports concerning the scope and adequacy of the internal control structure and procedures for financial reporting. This statement shall also assess the effectiveness of such internal controls and procedures.

The registered accounting firm shall, in the same report, attest to and report on the assessment on the effectiveness of the internal control structure and procedures for financial reporting.

## **3.8.3 IBM capability mapping**

To meet the challenges that are associated with Sarbanes-Oxley, an integrated compliance framework should include both of the following items:

- ▶ Documenting, evaluating, and reporting on business controls (document and manage)
- ▶ Enforcing those business controls through process automation (enforce)

You can identify the IBM Security Blueprint components and subcomponents that can help you attain compliance with SOX in a similar way as you can with PCI. Mostly, SOX requirements are applicable to a subset of your IT infrastructure components (servers and applications that handle and maintain financial data, ERP systems, and so on). In addition, most of the SOX requirements describe how to assure data integrity and control access to financial and asset-related data. Although these requirements sound basic, they can make a long list of necessary security capabilities.

For example, many capabilities are required in relation to *access control*. These capabilities include, among others, the implementation of entitlement management, possibly managed through an RBAC approach, real-time enforcement of access, controlling access of privileged users to the data, and so on. These access control related capabilities must be complemented by other indirectly related capabilities, for example, ensuring the integrity of the system that is hosting the concerned data because all access controls could possibly be circumvented by malware.

The IT systems that host SOX relevant data require many security capabilities, most of which can be described and designed by using the IBM Security Blueprint Foundational Security Management components and subcomponents.

### 3.9 Health Insurance Portability and Accountability Act

To improve the efficiency and effectiveness of the healthcare system, the Health Insurance Portability and Accountability Act<sup>11</sup> of 1996 (HIPAA), Public Law 104-191, includes *administrative simplification provisions* that require the US Department of Health and Human Services (HHS) to adopt national standards for electronic healthcare transactions and code sets, unique health identifiers, and security. At the same time, Congress recognized that advances in electronic technology could erode the privacy of health information. Then, Congress incorporated provisions into HIPAA that mandated the adoption of federal privacy protections for individually identifiable health information.

The US Department of Health and Human Services published a final Privacy Rule in December 2000, which was later modified in August 2002. This rule defines national standards for the protection of individually identifiable health information by three types of covered entities: health plans, healthcare clearinghouses, and healthcare providers who conduct the standard healthcare transactions electronically. Compliance with the privacy rule was required as of April 14, 2003 (April 14, 2004 for small health plans).

The HHS published a final Security Rule in February 2003. This rule defines national standards for protecting the confidentiality, integrity, and availability of electronic protected health information. Compliance with the Security Rule was required as of April 20, 2005 (April 20, 2006 for small health plans).

---

<sup>11</sup> For more information about HIPAA, see <http://www.hhs.gov/ocr/privacy/>.

Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA, known as the administrative simplification (AS) provisions, requires the establishment of national standards for electronic healthcare transactions and national identifiers for providers, health insurance plans, and employers.

The administrative simplification provisions also address the security and privacy of health data. The standards are meant to improve the efficiency and effectiveness of the nation's healthcare system by encouraging the widespread use of electronic data interchange in the US healthcare system.

### 3.9.1 Common strategy and terminology

Per the requirements of Title II, the United States Department of Health and Human Services promulgated five rules about administrative simplification:

- ▶ Privacy Rule
- ▶ Transactions and Code Sets Rule
- ▶ Security Rule
- ▶ Unique Identifiers Rule
- ▶ Enforcement Rule

### 3.9.2 Industry guidance and techniques

This section takes a closer look at these rules.

#### Privacy Rule

The HIPAA Privacy Rule regulates the usage and disclosure of Protected Health Information (PHI) that is held by *covered entities* (generally, healthcare clearinghouses, employer sponsored health plans, health insurers, and medical service providers that engage in certain transactions). By regulation, the Department of Health and Human Services extended the HIPAA privacy rule to independent contractors of covered entities who fit within the definition of *business associates*. PHI is any information that is held by a covered entity that concerns health status, provision of healthcare, or payment for healthcare that can be linked to an individual. This situation is interpreted rather broadly and includes any part of an individual's medical record or payment history. Covered entities must disclose PHI to the individual within 30 days upon request.

## Transaction and Code Sets Rule

HIPAA-covered health plans are now required to use standardized HIPAA electronic transactions. Information about this situation can be found in the final rule for HIPAA electronic transaction standards (74 Fed. Reg. 3296, published in the Federal Register on January 16, 2009).

Here are the Key Electronic Data Interchange (EDI)(X12) transactions that are used for HIPAA compliance:

- ▶ EDI healthcare Claim Transaction set (837)
- ▶ EDI Retail Pharmacy Claim Transaction
- ▶ EDI healthcare Claim Payment/Advice Transaction Set (835)
- ▶ EDI Benefit Enrollment and Maintenance Set (834)
- ▶ EDI Payroll Deducted and other group Premium Payment for Insurance Products (820)
- ▶ EDI healthcare Eligibility/Benefit Inquiry (270)
- ▶ EDI healthcare Eligibility/Benefit Response (271)
- ▶ EDI healthcare Claim Status Request (276)
- ▶ EDI healthcare Claim Status Notification (277)
- ▶ EDI healthcare Service Review Information (278)
- ▶ EDI Functional Acknowledgement Transaction Set (997)

## Security Rule

The Security Rule complements the Privacy Rule. Although the Privacy Rule pertains to all Protected Health Information (PHI), including paper and electronic, the Security Rule deals specifically with Electronic Protected Health Information (EPHI). It lays out three types of security safeguards that are required for compliance: administrative, physical, and technical. For each of these types, the rule identifies various security standards, and for each standard, it names both required and addressable implementation specifications. Required specifications must be adopted and administered as dictated by the rule.

## Unique Identifiers Rule (National Provider Identifier)

HIPAA covered entities such as providers that complete electronic transactions, healthcare clearinghouses, and large health plans, must use only the National Provider Identifier (NPI) to identify covered healthcare providers in standard transactions. The NPI is unique and national, never reused, and except for institutions, a provider usually can have only one. An institution may obtain multiple NPIs for different *subparts*.

## Enforcement Rule

On February 16, 2006, the HHS issued the latest rule about HIPAA enforcement. It became effective on March 16, 2006. The Enforcement Rule sets civil money penalties for violating HIPAA rules and establishes procedures for investigations and hearings for HIPAA violations.

### 3.9.3 IBM capability mapping

The HIPAA rules have a direct relationship to the IBM Security Blueprint. Some of them have a more straightforward relationship (Privacy and Security Rules), and some might be considered as *industry-specific* (Transaction and Code Sets and Unique Identifiers Rule).

- Privacy Rule

The problem that is solved in the HIPAA Privacy Rule, which regulates the usage and disclosure of Protected Health Information (PHI) that is held by covered entities, directly corresponds to the IBM Security Blueprint areas of Identity, Access, and Entitlement Management together with the Data and Information Protection Management.

- Transaction and Code Sets Rule

Although the Privacy Rule of HIPAA is directly related to the IBM Security Blueprint, the Transaction and Code Sets Rule shall be considered an industry-specific rule, without direct relationship to the IBM Security Blueprint.

- Security Rule

The Security Rule has the most IBM Security Blueprint coverage. We could also say that although HIPAA differentiates between Privacy and Security Rules (in the HIPAA naming convention meaning), from an IBM Security Blueprint perspective those two rules cover similar areas. As described in “Security Rule” on page 141, the Security Rule complements the Privacy Rule, with more focus on the electronic protected health information (EPHI). Based on this fact, you can consider the same IBM Security Blueprint components to be in direct relationship with the Security Rule, namely, Identity, Access, and Entitlement Management (complements HIPAA 164.308) together with the Data and Information Protection Management. The IBM Security Blueprint Physical Security component matches the HIPAA Security Rule 164.310. The IBM Security Blueprint Security Policy Management can be mapped to the HIPAA 164.136 policies and procedures.

- Unique Identifiers Rule

The Unique Identifiers Rule defines a set of unique identifiers that are divided into four classes, where the National Provider Identifier is one among them. This rule is a purely industry-specific registry and dictionary, and there is no specific mapping between the Unique Identifiers Rule and the IBM Security Blueprint.

- Enforcement Rule

The Enforcement Rule is strictly an industry-specific rule that is related only to HIPAA. Although it describes various ways of the HIPAA enforcement, such as penalties and hearings, it makes no sense to map it to any part of the IBM Security Blueprint.

## 3.10 Conclusion

This chapter provided a concise overview of some of the well-known information security-related frameworks, standards, and regulations. As there is no silver bullet for a security architecture or solution approach, you see that each of those frameworks, standards, and regulations has a certain focus or follows a specific approach, and more than one can be used in an organization.

For each of these items, we described how the IBM Security Blueprint and its components relate to the individual framework and how they can be used by organizations that implement any of those frameworks or comply to any of the mentioned regulations.







## Using O-ESA to develop an enterprise security architecture

The IBM Security Blueprint can help you identify the necessary security services and related subcomponents to develop a security solution for your organization. But defining the required security capabilities is just a first step. Before you can deploy software-based solutions, design policies, or define zones in your network, you must create an architecture. So, instead of starting immediately with the detailed design per component, you should define an overarching *enterprise security architecture* (ESA) to set the context and constraints for the technical designs. This chapter uses the *Open Enterprise Security Architecture* (O-ESA) from the Open Group (reference catalog number G112, April 2011) to describe an approach about how an ESA can be created from the IBM Security Blueprint.

The first section provides a summary of O-ESA. For more information, go to:

<https://www2.opengroup.org/ogsys/jsp/publications/PublicationDetails.jsp?publicationid=12380>

This chapter includes the following sections:

- ▶ Introduction to O-ESA
- ▶ Alignment of the IBM Security Blueprint and O-ESA
- ▶ O-ESA based approach to develop an enterprise security architecture
- ▶ Conclusion

## 4.1 Introduction to O-ESA

The O-ESA is a policy-driven security architecture that places this architecture in the context of a larger enterprise security program and describes the major elements of an ESA: *Governance*, *Technology Architecture*, and *Operations*.

An enterprise security architecture must be created at the level of the overall corporation, and thus in relationship with the *enterprise architecture*, the *corporate risk management* guidelines, and IT governance as defined within the organization. As such, the ESA is the part of an enterprise architecture that defines how to fulfil the objectives of preserving the availability, integrity, and confidentiality of an organization's information.

Enterprise security architecture is the specialized framework for fulfilling these objectives while it satisfies the security demands placed on the IT service organization by its customers. It includes all aspects of security governance, security technology architecture, and security operations that are required to protect the IT assets of the enterprise.

The O-ESA Enterprise Security Program is expanded into four concentric rings of responsibility (Figure 4-1):

- ▶ Overall Program Management responsibility in the outer ring
- ▶ Governance responsibility in the second ring
- ▶ Architecture, or Technical Architecture, in the third ring
- ▶ Operations responsibility in the inner ring

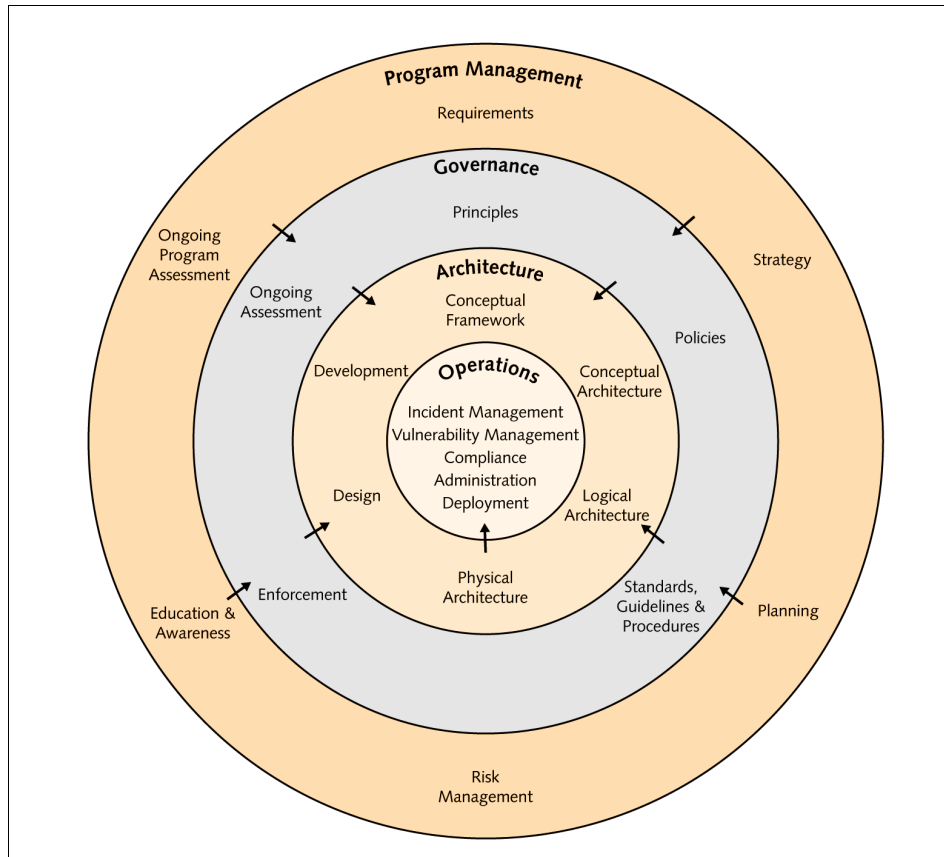


Figure 4-1 O-ESA Enterprise Security Program (© The Open Group)

Each ring identifies key components and processes that fall within that responsibility domain. The components of each ring represent deliverables that further narrow the definition of what must be provided by the inner rings. The Requirements, Strategy, Planning roadmaps, Risk Management assessments, Education and Awareness, and the Ongoing Program Assessment from the outer Program Management ring narrow the definition of what must be provided in the governance, technology, and the architecture rings.

Here are the functions of O-ESA components and processes:

- ▶ Security Governance
  - Principles: Basic assumptions and beliefs that provide overall security guidance.
  - Policies: The security rules that apply in various control domains.
  - Standards, Guidelines, and Procedures: The implementation of the policies through technical requirements, recommended practices, and instructions.
  - Enforcement: The processes for ensuring compliance with the policies.
  - Ongoing Assessment (audit): The process of reviewing security activities for policy compliance.
- ▶ Security Technology Architecture
  - Conceptual Framework: Generic framework for policy-based management of security services.
  - Conceptual Architecture: Conceptual structure for management of decision-making and policy enforcement across a broad set of security services.
  - Logical Architecture: Provides more detail about the logical components that are necessary to provide each security service.
  - Physical Architecture: Identifies specific products, showing where they are, and how they are connected to deliver the necessary functionality, performance, and reliability.
  - Design and Development: Guides, templates, tools, reusable libraries, and code samples to aid in the effective usage and integration of applications into the O-ESA environment.
- ▶ Security Operations
  - Incident Management: The process for responding to security-related events that indicate a violation or imminent threat of violation of the security policy.
  - Vulnerability Management: The process for identifying high-risk infrastructure components, assessing their vulnerabilities, and taking the appropriate actions to control the level of risk to the operational environment.
  - Compliance: The process for ensuring that the deployed technology conforms to the organization's policies, procedures, and architecture.
  - Administration: The process for securing the organization's operational digital assets against accidental or unauthorized modification or disclosure.

- Deployment: Assumed to be the normal IT deployment process, not a security operations process.
- Services: The core security functions that are defined by the security technology architecture that support devices and applications and other security operations processes.
- Devices and Applications: Devices and applications that use O-ESA services and are supported by the security operations processes.
- Event Management: The process for day-to-day management of the security-related events that are generated by various devices across the operational environment, including security, network, storage, and host devices.

## 4.2 Alignment of the IBM Security Blueprint and O-ESA

Defining an enterprise security architecture is not a one-time activity. Setting the foundation takes the most time and effort, but after it is defined, it requires regular updates that are driven by the changes in business requirements, possibly new threats, or disruptive changes in technology. Although the CISO office cannot play an active role in all security-related activities in an organization, it must own the Enterprise Security Program and participate as a stakeholder in the related activities.

Figure 4-2 shows the O-ESA Enterprise Security Program Framework. In this framework, the CISO office must fulfill its role in several activities, and this role varies depending on the type of activity.

**Nomenclature:** In the O-ESA figures, the rectangular boxes represent components or deliverables, and the rounded boxes represent processes.

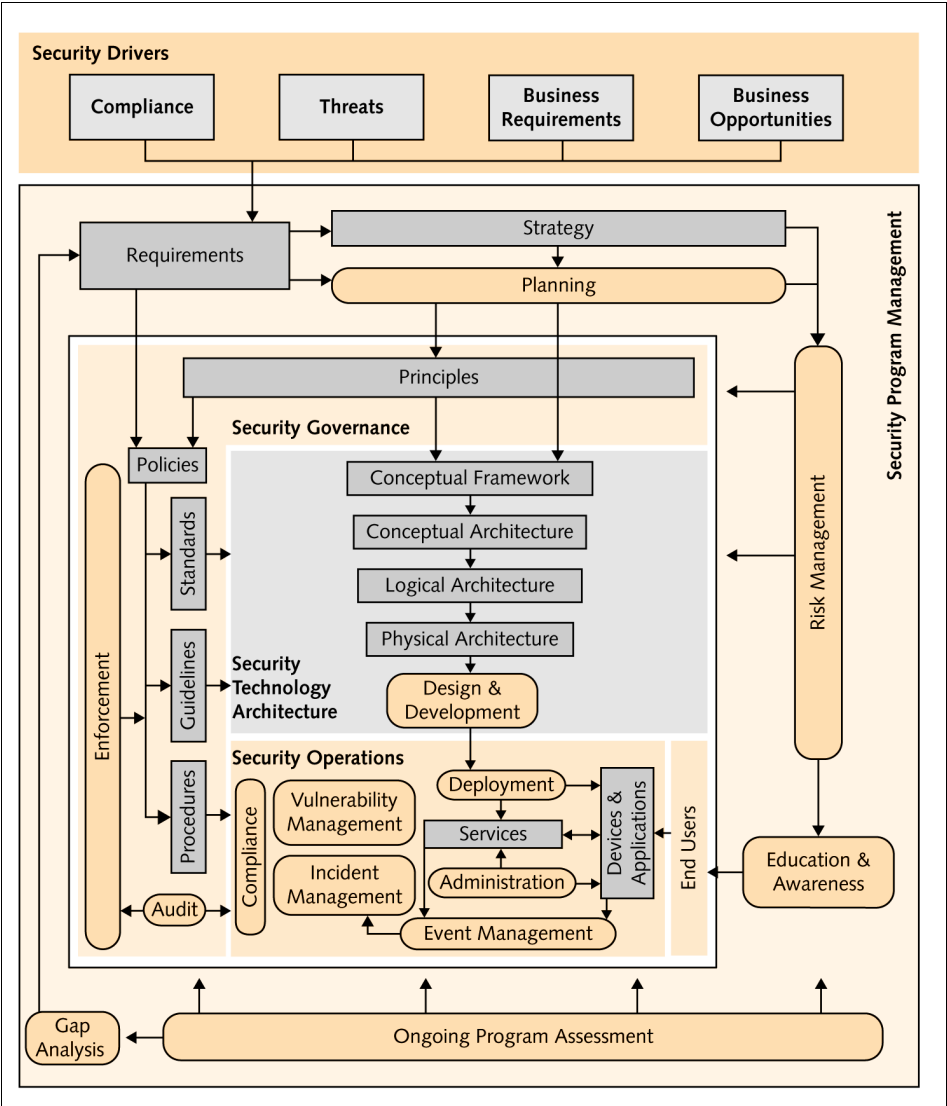


Figure 4-2 O-ESA Enterprise Security Program Framework (© The Open Group)

Here are the security activities where the CISO office should play a role:

- ▶ Security Program Management
  - Define requirements.
  - Validate requirements.
  - Define strategy and high-level planning.
  - Drive or participate in the Risk Management activities.
  - Run Education and Awareness programs for users.
  - Assess the effectiveness of the implemented security services and identify possible gaps.
- ▶ Security Governance
  - Define principles (the IBM Security Framework can possibly be used to define the organization's security principles in the four domains).
  - Define Policies and procedures.
  - Guide and monitor the translation of policies into Guidelines and Standards.
  - Perform an audit and facilitate external audits.
  - Define and run a policy enforcement program (and be the process owner).
- ▶ Security Technology Architecture
  - Provide input to the architecture team.
  - Validate the deliverables for compliance with policies and guidelines.
- ▶ Security Operations
  - Have day-to-day follow-up of overall security metrics and KPIs.
  - Decide and adapt an incident severity classification (at time of review or at time of demand).
  - Coordinate incident response actions for severe incidents.
  - Review reports.
  - (Re)act upon severe out-of-compliance situations.

The IBM Security Blueprint can help organizations define their security strategy based on the seven Foundational Security Management components and the interaction with the two service management components. For each foundation service, you must select the subcomponents that provide the needed Security Services and Infrastructure subcomponents. This representation can provide the means to frame the security program.

To evolve from the IBM Security Blueprint to an enterprise security architecture, you can use the Foundational Security Management components closed loop (see Figure 4-3). This model can be adapted and extended to realize alignment with O-ESA. The closed loop representation for the Foundational Security Management components is described in 2.1, “Foundational Security Management” on page 32.

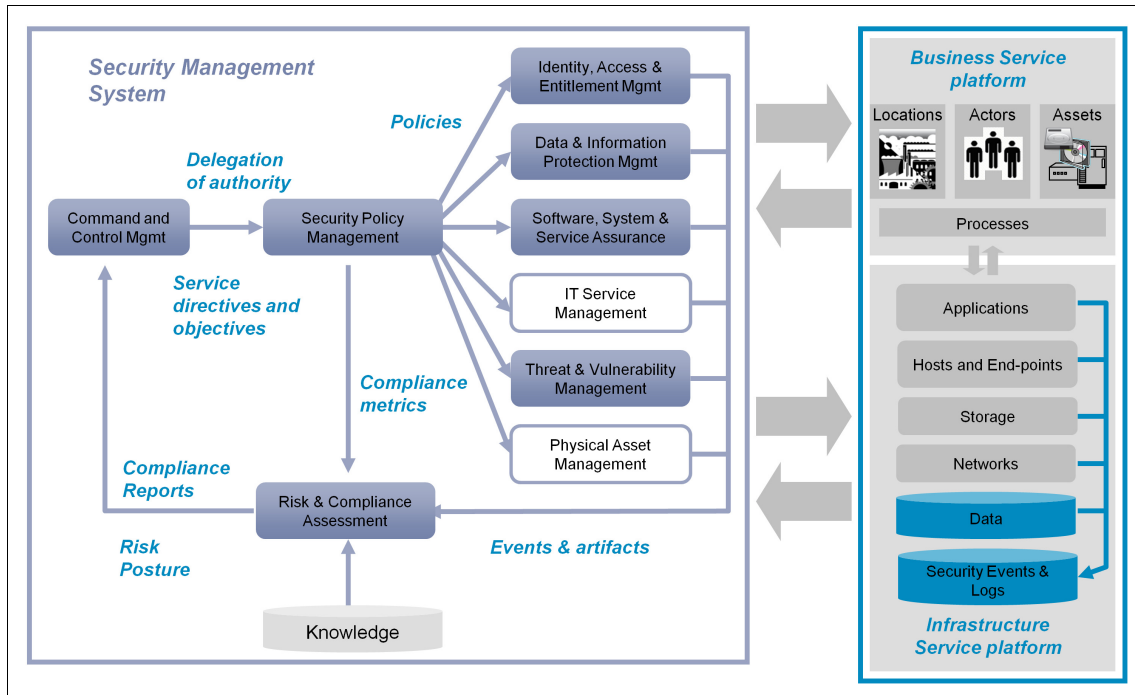


Figure 4-3 Foundational Security Management components closed loop

To align the Foundational Security Management components' closed loop with the O-ESA model, the closed loop must be extended to incorporate all the security governance activities of O-ESA:

- ▶ Definition of the principles.
- ▶ Addition of the audit activity.
- ▶ Translation of security policies into guidelines, procedures, and corporate standards.
- ▶ Policy enforcement program.
- ▶ Education and awareness.



- Risk and compliance are covered in the following activities: Risk Management (Security Program), Compliance Assessment (Security Operations), and Audit (Security Governance). Knowledge in this context can be further described as “Standards & Legislation” and “Threat Catalogue”.

Besides an extension of the Foundational Security Management components closed loop within the Governance domain, there are also related activities at the program management level. Recall that O-ESA has a constraint-driven approach, so security Program Management sets the context and the boundaries where these Governance activities are performed.

Adding these activities and reusing the distribution between Program Management and Governance results in the merged model that is shown in Figure 4-4 and Figure 4-5 on page 154. The dotted line represents the information that is provided by the *event management* component that is shown in Figure 4-5 on page 154. The Command and Control Management team obtains situational awareness about possible security incidents and threats as reported by the event management component. The same component also provides reporting capabilities on compliance and other specific audit-related reports.

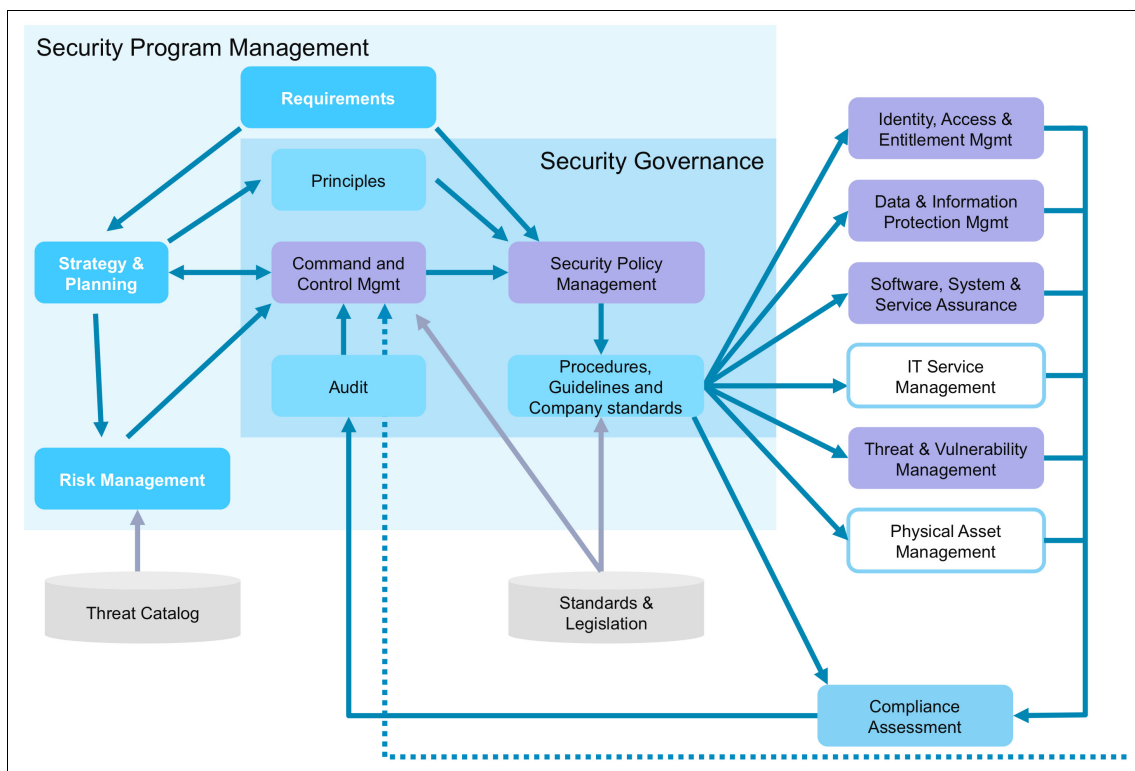


Figure 4-4 Foundational Security Management components closed loop - O-ESA integration

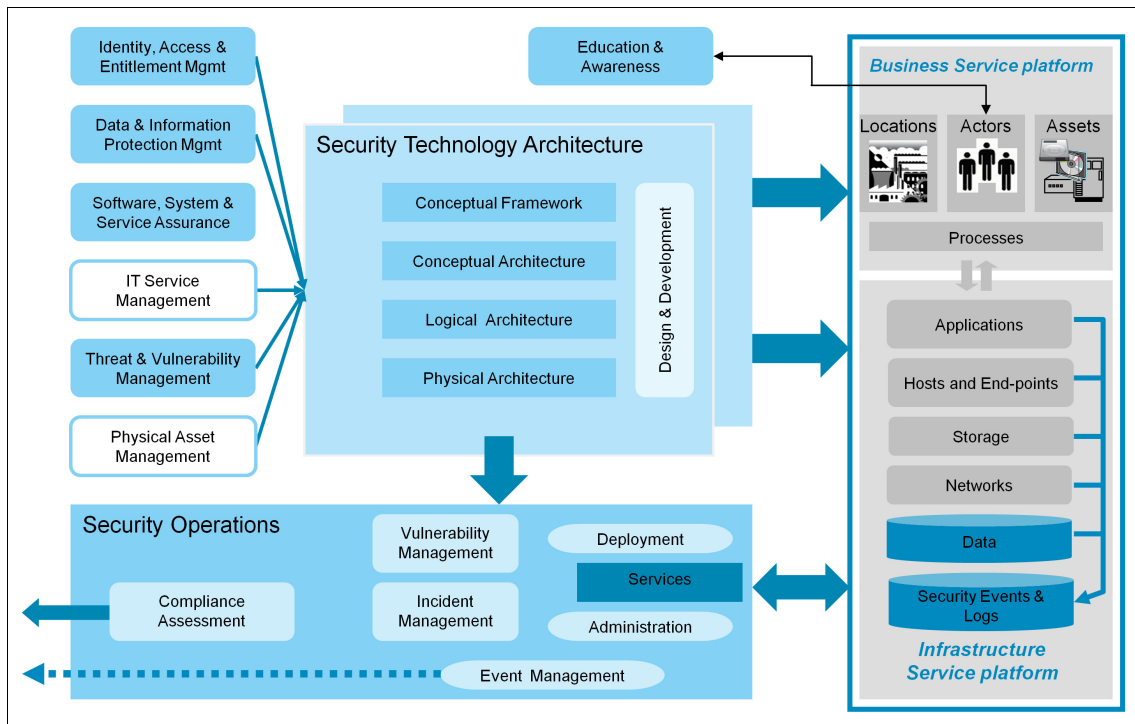


Figure 4-5 Security Technology Architecture

The gathering of security requirements is not described here. There are other publications that describe how different sources of requirements (such as compliance, threats, and business) can drive both the security strategy and the definition of the security policies, and by consequence, the corresponding security architecture. For example, the SABSA framework (described in 3.4, “Sherwood Applied Business Security Architecture” on page 120) describes how requirements can be gathered. In a regular architecture, the security aspects of the solution are mostly categorized as *non-functional requirements*, while in an ESA all security requirements are core *functional requirements*.

The CISO office, which is assumed to perform a major role in the Command and Control Management service, both generates and validates those requirements. The security policy management service manages the policy lifecycle and provides more granular instructions in the form of procedures and guidelines. Those policies are grouped per Foundational Security Management component and provide the input for the architecture (Figure 4-5).

The Security Technology Architecture describes how the policies, guidelines, and standards are translated into a technology solution. The architecture must define how and where the security controls (for example, through policy enforcement points (PEP)) to both the business processes and the infrastructure layer are implemented. For the processes, the control might be an extra manual action or even a change to the process. In the infrastructure layer, these controls are realized through appliances and applications.

In parallel, you must, through the architecture, define how the security operations can be augmented with the new or updated security services. This step must be implemented for all aspects of operations, including the deployment and daily management of the security services and the management of the events and information that are generated by the service. The security incident management process, and the list of endpoints that must be scanned for vulnerabilities or assessed for compliance to the policies, might have to be updated.

Security architecture is not the only factor that impacts the behavior of the user. As part of the Program Management, the Education and Awareness activity is meant to change and drive user behavior.

O-ESA introduces a *conceptual framework* for policy-driven security. Similar to the XACML standard for authorization, the concepts of the Policy Repository, Policy Decision Point, and Policy Enforcement Point are used for all security services (that is, auditing, content control, and so on). This conceptual framework in O-ESA represents the starting point for conceptual architecture.

The conceptual architecture groups security services per policy management domain. Each domain can have ideally one policy decision point (PDP) (in reality, there can be several PDPs per domain) and a corresponding policy repository. The security policies are enforced by the policy enforcement points (PEP) at the different layers in the infrastructure, as shown in Figure 4-6. The figure shows the conceptual architecture for the Threat and Vulnerability Management component, which results in one or more policy repositories (in O-ESA, these repositories fit into the configuration management administrative domain) and the corresponding PDP and PEPs that are deployed at the different layers of the IT infrastructure (for example, the agents that are used to scan for vulnerabilities).

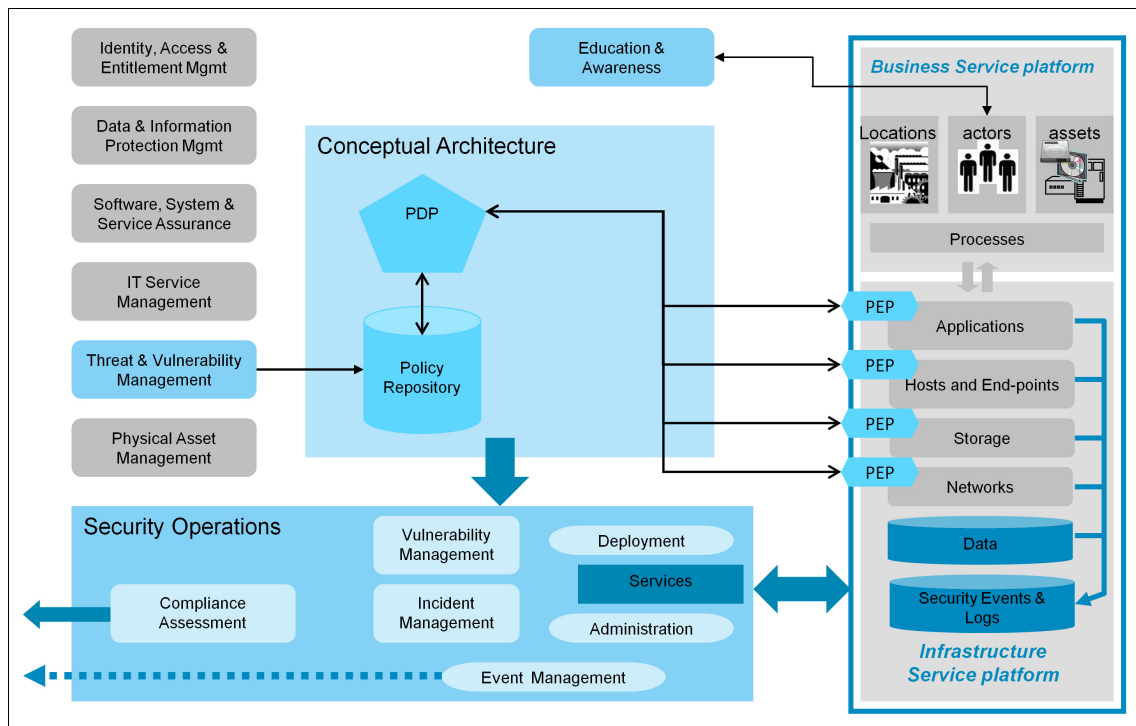


Figure 4-6 Conceptual architecture

## 4.3 O-ESA based approach to develop an enterprise security architecture

This section takes a closer look at the following topics:

- ▶ Introduction
- ▶ Governance
- ▶ Architecture
- ▶ Operations

### 4.3.1 Introduction

Here are the individual steps that are needed to define an enterprise security architecture:

1. Requirements gathering.
2. Define the strategy and policies that are based on the requirements (program management and governance).
3. Define the security domains (logical architecture).
4. Define the security services placement in the security domains.
5. Define the component model for the security services (logical architecture).
6. Define the use cases for the security services (logical architecture).
7. Define the operational model for the security services (physical architecture).
8. Define the security operations for the concerned security services (security operations).
9. Validate the architecture and perform a risk assessment that is based on anomalous flows (risk management).

When you create an enterprise security architecture, many of the elements might be present and implemented already in an organization, although they might not be fully documented or governed through an enterprise-wide architecture. So, although some of the steps are listed for completeness, they can be skipped if any of them are implemented already.

#### **Requirements gathering (Program Management)**

The requirement gathering phase is not described further in this publication. O-ESA refers to the most common security drivers as input for requirements, compliance (both with external regulations as organizational standards), threats (based on an ever evolving threat catalog), and business requirements and opportunities.

## **Defining a strategy and policies from the requirements (Program Management and Governance)**

This step involves two subtasks:

- ▶ **Strategy**

Select security services from the IBM Security Blueprint to build an organization-specific security services catalog. Select or add subcomponents if necessary. Define whether any of these security services are mandatory or wanted, and describe how projects in the organization can use these services.

- ▶ **Policies**

If not done previously, you must define security policies for the organization and use existing templates, such as ISO 27002. For any existing policies, a regular review should be planned and policies should be updated because of any changes in the environment.

## **Defining security domains (Architecture)**

Here you define a set of security domains that your organization uses for their services operation. For example, you can segregate your environment into the following security domains:

- ▶ Uncontrolled
- ▶ Controlled
- ▶ Restricted
- ▶ Secured
- ▶ External Controlled

The definition of these domains and their boundaries are typically driven by information classification and control objectives.

## **Defining security services placement in the security domains**

The systems with the same classification or control objectives are grouped in domains. Information crossing the domains is subject to specific security controls when applicable. The earlier selected security services are materialized by the policy enforcement points that are deployed within the infrastructure. These PEPs must be deployed within the different security domains, and some PEPs are specific to the domain boundaries. All systems and applications already provide security controls. It is important that these controls are configured in accordance with the security policies. Specific security services (for example, a Secure Token Service) can complement the default controls that come standard with systems and applications.

## Defining a component model for the security services (Logical Architecture)

Similar to component modeling, the security services attributes are defined from a functional perspective. In the operational model, the technical aspects of the services are defined. The list of attributes might differ depending on the type (boundary control, encryption, user activity monitoring, and so on), but most common attributes can be collected by using the example form that is shown in Table 4-1.

Table 4-1 Security Service Description form

Security Service Description					
Security service name:		Version number:		Foundation service:	
Services to provide:		Service owner:		Service consumers:	
Policies to support:		Security domains to deploy:		Is it a boundary control:	
Service level objectives:					
IT components:					
Policy management (including policy data):		Policy decision points:		Policy enforcement points:	
Which type of data is it protecting (if applicable):					
At rest:		In motion:		Highest allowed classification:	

## Defining use cases for the security services

The goal for this activity is to document the most common use cases for the relevant security services. This activity is especially useful for those services that provide direct benefits to the business, for example, authentication services for users, partners, and employees. For security services, such as intrusion detection, the description can be kept concise and focused on the security operation aspect.

## **Defining an operational model for security services (physical architecture)**

In an enterprise security architecture, the operational model can remain at a fairly high level. This operational model can cover high-level decisions for the deployment of security services in the infrastructure. These high-level decisions, for example, can describe the selected technology, the approach that is taken for high availability and disaster recovery, and network diagrams. During the detailed design phase, descriptions are provided about how the different components of a security service must be configured and deployed in the infrastructure.

## **Defining security operations for the relevant security services**

Deploying a security service within an organization is just the first step. The security operations must ensure its correct deployment and day-to-day functioning. These tasks are a top priority from the risk management aspect. For example, an endpoint can potentially become a high risk factor for the organization if it is not correctly monitored because of a misconfigured component, failing security services, or the endpoint not being listed as a target in the asset management discipline. These reasons are why a coordinated approach should be defined in alignment with the security policies and the IT Service Management of the organization, while you define an enterprise security architecture.

## **Validating architecture and performing a risk assessment that is based on anomalous flows**

Good vulnerability management starts during requirement gathering and continues through the different phases while you build the architecture. In this task, the different security services should be evaluated and validated against possible malicious activity, both internally and externally. This validation should be repeated as part the detailed design phase later on.

### **4.3.2 Governance**

The goal of security governance in an enterprise security architecture is to define and enforce how security is deployed and maintained to reduce the identified risks to an acceptable level. Governance provides direction to the organization's management about how to realize the required security program within the enterprise. O-ESA defines the following components for the security governance activity:

- ▶ Principles
- ▶ Policies



- ▶ Guidelines
- ▶ Standards
- ▶ Procedures

The enforcement and audit processes help you ensure that the policies are enforced and measured against compliance and effectiveness.

You can safely assume that many organizations already have security policies in place. The degree to which these policies are translated into guidelines and procedures vary from one organization to another. To define security policies, several templates are readily available, with ISO 27002:2005 being one of the most used. This section lists some general elements of importance to the security governance task. More information can be found in the O-ESA handbook and the ISO standard.

### **Establishing a formal governance board function**

The way security governance is implemented differs from one organization to another. To fully endorse governance, a board is needed that steers and validates all aspects of security governance. Possible board participants can be the Risk Manager, Corporate Information Security Officer, Internal Audit, a representative of the CIO office, Enterprise Architect, and Enterprise Security Architect. Often, you also find representatives from the business line management that participate in governance board activities. The Enterprise Architect typically is always on this board.

### **Identifying the guiding principles**

Select and define the principles that are applicable to your organization. In both the O-ESA publication and in this publication, there are principles that are listed that can be used to compile an organization-specific set of principles. These principles provide the highest level of guidance.

### **Security policy definition**

Several existing publications can and should be used for this step. We have already referred to the ISO 27002 standard, but there are other sources available as well. For example, NIST and the Information Security Forum (ISF) provide publications that can be used for this purpose.

### **Implementing the policies**

This step requires the definition of guidelines, organizational standards, and procedures (the so-called *standard operating procedure* (SOP)). Several resources are available to support this activity, which is mostly industry-specific (for example, HIPAA and PCI DSS).

Some of the procedures can depend on the selected technology and, as a consequence, the final details of the procedure can be completed only after the technology is selected and tested.

### **Implementing the processes for enforcement and ongoing assessment**

Defining policies and procedures have no meaning if there are no processes in place to enforce the defined policies and measure the effectiveness and completeness through regular audits. An ongoing assessment must ensure that the security policies stay up to date and remain in line with the evolving business requirements and anticipate any possible new type of risks.

## **4.3.3 Architecture**

Here are the different activities in the Architecture task:

- ▶ Use the O-ESA conceptual framework where applicable to define the elements of the selected security services.
- ▶ Describe the security service functionality as part of the logical architecture.
- ▶ Define the physical architecture. Where should it be deployed and how must it be configured?
- ▶ Describe the use cases that the security services must support.
- ▶ Define the required actions as part of the security operations (as explained in 4.3.4, “Operations” on page 169).
- ▶ Validate the objectives that are defined in the security policies.

This section describes the following activities:

- ▶ Definition of the security domains
- ▶ Security service description and corresponding use cases
- ▶ Placement of the IT components of a security service in the domains
- ▶ High level physical architecture

Figure 4-7 shows the activities for the technical architecture.

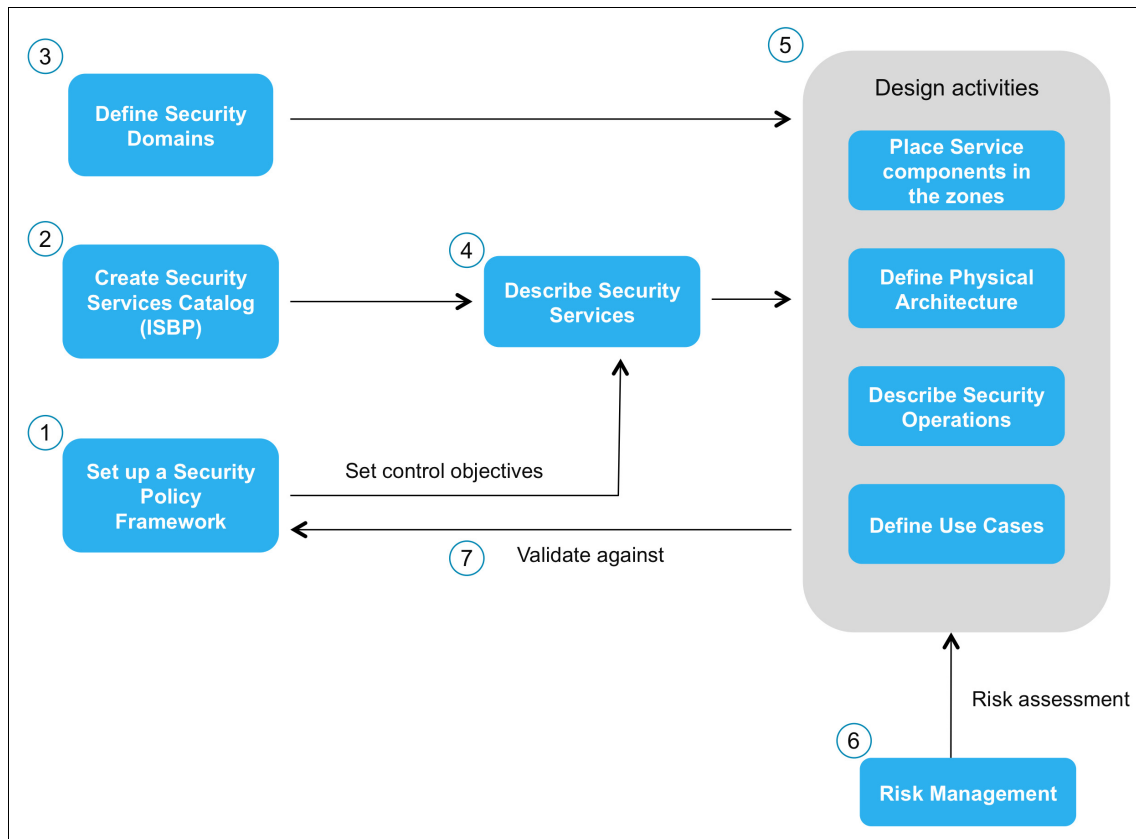


Figure 4-7 Steps to develop the technology architecture of an ESA

## Security domains

Most organizations define and set up different security domains in their (network) infrastructure. During an enterprise security architecture project, you must take this reality into account by either validating or defining the necessary changes to the existing implementation. These changes can imply the creation of new zones, consolidation of existing zones, or changes to the boundary controls between zones.

This section briefly describes the approach for the definition of the security domains and the corresponding network zones. Only the high-level steps are mentioned here; more information can be found in *Enterprise Security Architecture Using IBM Tivoli Security Solutions*, SG24-6014.

The *uncontrolled* zone refers to anything outside the control of an organization. Access from the uncontrolled environment to systems in the controlled zone could be implemented by using a wide array of channels.

The *controlled* zone restricts and regulates access between an uncontrolled and a restricted (a traditional DMZ) zone.

In a *restricted* zone, access is tightly controlled and restricted. Only authorized individuals are granted access and there is no direct communication that is allowed to external sources (Internet).

In a *secured* zone, access is available only to a small group of highly trusted users. Access to one secured area does not necessarily grant access to another.

An *external controlled zone* represents a zone that is controlled by a business partner organization in which data is stored (for example, credit reporting agencies, banks, and government agencies). This data might require a different set of controls to maintain a sufficient level of trust.

Components requiring the same level of control or protection can be grouped and placed in one zone. Data classification also plays a role in defining security domains and component placement within those domains. Systems hosting data with the same (high) level of classification are grouped. The boundary security controls must enforce policies (allow data to pass or not and if so under which condition, for example, encrypted during transit).

Figure 4-8 shows a sample representation of security domains.

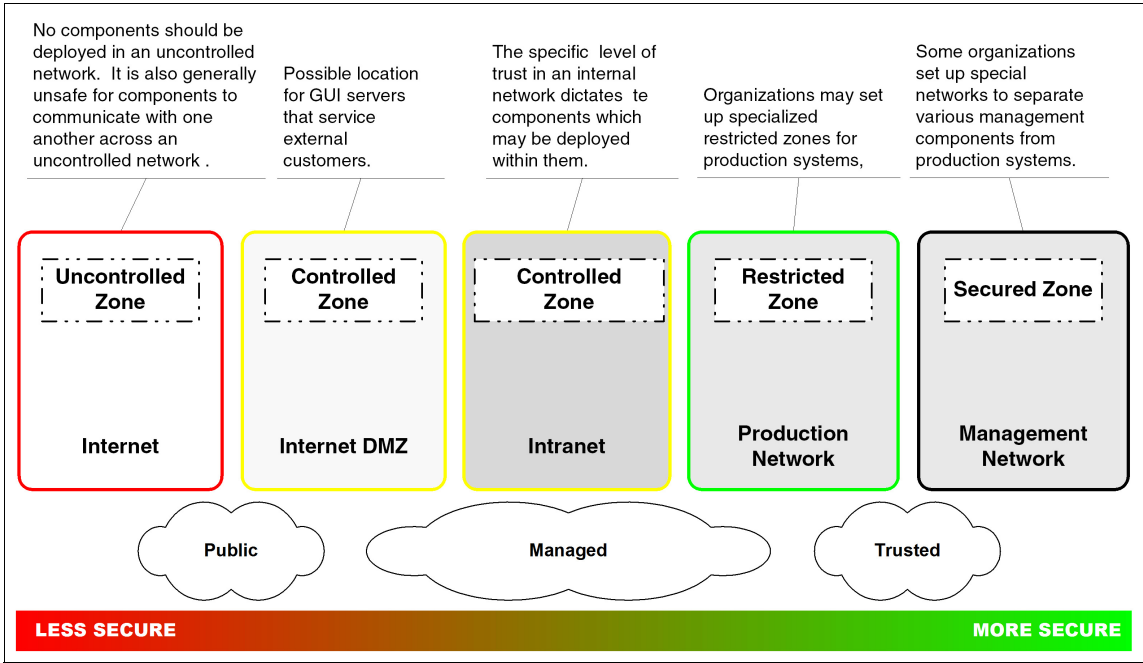


Figure 4-8 Sample representations of security domains

### Security services description

For each selected security service, the attributes, scope, and functionality must be defined. The example form that is shown in Table 4-1 on page 159 can be used to collect and document this information. When the deployment is diverse or large, consider using a form with a reduced scope.

Let us use the authentication service as an example. From a generic perspective, it is clear that authentication is required to access several systems and data sources. This control must be deployed for different types of users (for example, employees, customers, and business partners) and at different layers of the infrastructure (for example, building, data center, server rack, operating systems, network components, middleware, applications, web services, and files).

Using this example, two forms are completed, shown in Table 4-2 and Table 4-3 on page 167. The first form covers an example about data protection for data at rest within the scope of employee's notebooks. The second example covers single sign-on (SSO) for privileged users.

*Table 4-2 Security Service Description Form - data protection*

Security Service Description					
Security service name:	Data encryption of data in rest	Version number:	Version 1.0	Foundation service:	Data and Information Protection
Services to provide:	<ul style="list-style-type: none"> <li>► Encryption of the entire notebook hard disk</li> <li>► Encryption Key recovery procedure</li> </ul>	Service owner:	CISO	Service consumers:	Employees
Policies to support:	Data protection policy	Security domains to deploy:	All employee's notebooks	Is it a boundary control:	No
Service level objectives:	<ul style="list-style-type: none"> <li>► Provide encryption capabilities to all employees with notebooks (100% attainment in 6 months).</li> <li>► A key recovery procedure must be available 24x7 in case employees forget their key-phrase.</li> <li>► A key recovery procedure for the decryption of notebooks of employees who left the company must be available.</li> </ul>				
IT components					
Policy management (including policy data):	Centrally defined policy that defines how the software is installed (no modifications allowed)	Policy decision points:	Part of the local agent	Policy enforcement points:	Local agent to be deployed on the notebooks

Security Service Description					
Which type of data is it protecting (if applicable)					
At rest:	<ul style="list-style-type: none"> <li>► Company confidential data</li> <li>► Personally identifiable information</li> </ul>	In motion:	Not applicable	Highest allowed classification:	Company confidential

Table 4-3 Security Service Description Form - SSO privileged users

Security Service Description					
Security service name:	Single sign-on	Version number:	v1.0	Foundation service:	Identity, Access, and Entitlement Management
Services to provide:	Provide SSO for privileged users	Service owner:	IT Infrastructure Manager	Service consumers:	Privileged users
Policies to support:	Control and monitor access of privileged users	Security domains to deploy:	Employee workstations from where privileged users access servers in Data Center	Is it a boundary control:	No
Service level objectives:	24x7 availability + fall back procedure if there is a failure (for example, envelope procedure) to ensure access to servers				
IT components					
Policy management (including policy data):	Central policy for: <ul style="list-style-type: none"><li>► Passwords for privileged users</li><li>► Access control to servers</li></ul>	Policy decision points:	Centrally managed with a local copy at the local agent on the workstation	Policy enforcement points:	Local agent on the workstation

Security Service Description					
Which type of data is it protecting (if applicable)					
At rest:	Passwords	In motion:	Password transmission is controlled by the application or the terminal session	Highest allowed classification:	Not applicable

### Physical Architecture

One of the first steps during the Physical Architecture task is the selection of the technology, which is far beyond the scope of this book. The selected technology must be deployed through software installation, installation of appliances, network devices, or a combination of all these solution types. Although the definition of the correct security policies and supporting security services is important, the correct and detailed design, configuration, and deployment of the corresponding technology is equally important.

The architecture should handle the following topics (non-exhaustive list):

- ▶ Identify and document the server components, network components, and workstation/endpoint components for the policy management, policy decision, and policy enforcement capabilities.
- ▶ Identify and document the interfaces between the components and communication details (ports and protocols).
- ▶ Address the non-functional requirements, such as availability, systems management, and disaster recovery.
- ▶ Identify and document the integration with other security services, for example, security information and event management (SIEM).
- ▶ Identify and document the test plans.

### Use cases

Describing the use cases helps you define, test, and later implement the functionality that must be provided by the security service. For example, these use cases are needed for user interactivity with the security services, such as authentication. The use cases also serve as a base for defining the test cases for user acceptance or, more precisely, acceptance of the delivered functionality by the solution.



## Validation

The validation of the architecture covers two major aspects:

- ▶ One is the verification if the design goals are reached. These goals are articulated in the security policies and in the functional requirements that come from the business line. This step should be one of the first activities of the test plan.
- ▶ The second validation should be done based on anomalous flows. By using realistic *what if scenarios*, possible shortcomings in the architecture can be revealed, or further improvement in protection be reached.

Both aspects of validation continue to play a role during the further iterations of the solution deployment and the corresponding test activities (system integration tests, user acceptance tests, operational tests, and so on).

### 4.3.4 Operations

Operations, also referred to as Security Operations, is the third pillar, or the center, of the O-ESA framework (shown in Figure 4-1 on page 147) that defines both the components and processes that are required for operational support of a policy-driven security environment (see Figure 4-9).

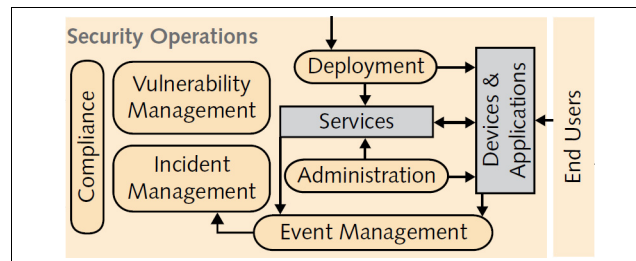


Figure 4-9 O-ESA Security Operations (© The Open Group)

The required processes are defined by the Security Operations function, which is split into two main categories. One category focuses on management controls (Security Compliance, Security Administration, and Asset Management), and the other category focuses on operational security controls (Event Management, Incident Management, and Vulnerability Management).

Figure 4-10 shows the O-ESA Security Operations model overview.

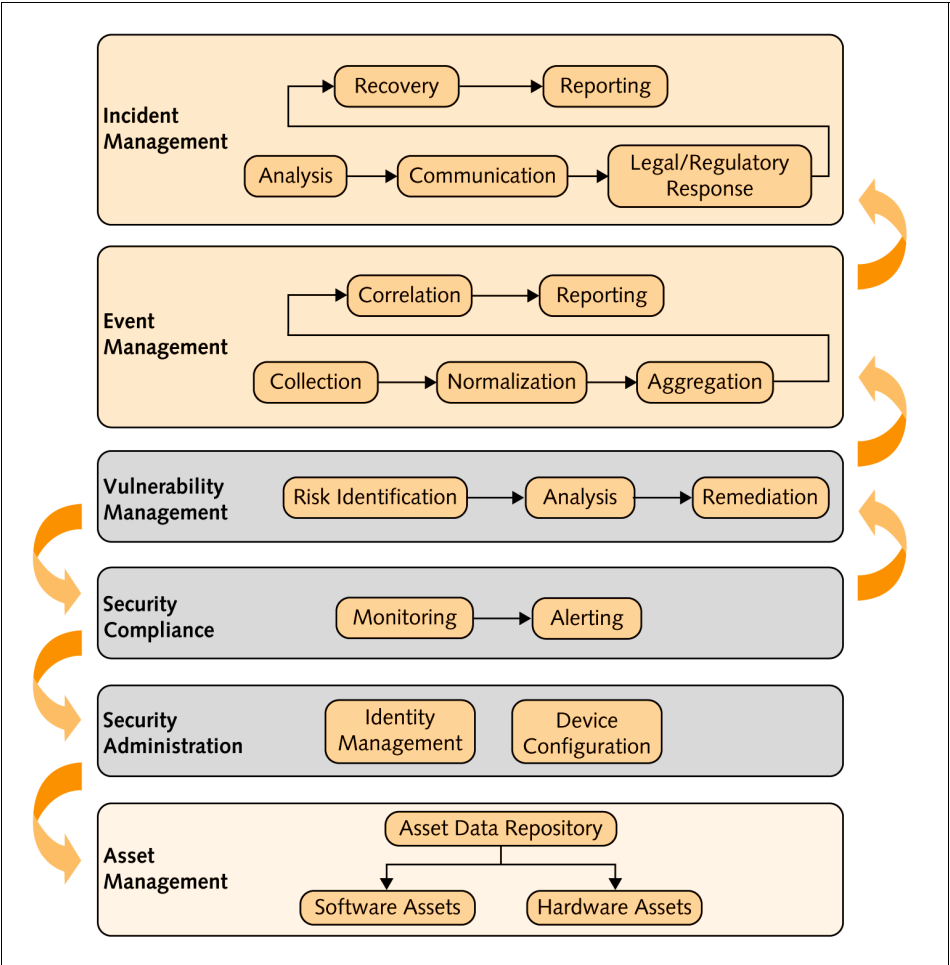


Figure 4-10 O-ESA Security Operations overview (© The Open Group)

The Security Operations model of the O-ESA can be extended to include the seven Foundational Security Management components and the two supporting service management components of the IBM Security Blueprint. By combining the Foundational Security Management components together with operational support processes, you can describe specific security operations, which come together as a set of activities and tasks that are designed to accomplish a specific control. The Foundational Security Management components with a focus on security operations and the actors that are involved are briefly described in the following sections.

## **Physical Asset Management**

Physical Asset Management in the context of Security Operations has the following characteristics:

- ▶ The objectives are to perform software and hardware asset management, including the discovery and inventory of network devices, networks, data storage, and application software.
- ▶ Activities include configuration management controls that track and record the individual posture of the assets.
- ▶ Process activities consist of asset verification, configuration control, administration, and planning.
- ▶ The actors that are involved in this control are the CISO, the asset owners, the auditors, and users.

Vulnerability management is linked to asset management, and configuration management is a subcomponent of the Threat and Vulnerability Management component.

## **Threat and Vulnerability Management**

Threat and Vulnerability Management has the following characteristics that relate to Security Operations:

- ▶ The goal is to monitor technical controls that track and record threats and vulnerabilities.
- ▶ Process activities include the identification of vulnerabilities in deployed systems, the determination of security threats, the follow-up of security-related information from various internal and external sources, and taking an appropriate response to control the level of risk to the operational environment.
- ▶ The actors that are involved in this control are all IT operations roles.

## **Identity, Access, And Entitlement Management**

The Identity, Access, And Entitlement Management component has the following characteristics that relate to Security Operations:

- ▶ Monitor the technical controls to realize the identity provisioning, identity lifecycle management, and access and authorization controls.
- ▶ Process activities include verification, policy configuration control, and administration and planning.
- ▶ The actors that are involved in this control are IT operations roles, IT service support roles, the auditors, and users.

## **Risk and Compliance Assessment**

The Risk and Compliance Assessment component has the following characteristics that relate to Security Operations:

- ▶ Monitor the controls that are run as part of the day-to-day risk management activities.
- ▶ Process activities include fraud detection, technical compliance monitoring, and tracking and reporting.
- ▶ The actors that are involved in this control are IT operations roles, IT management roles, the auditors, and the risk officer.

## **IT Service Management**

The IT Service Management component has the following characteristics that relate to Security Operations:

- ▶ Monitor the IT Service Management processes, such as change and release management, and event and incident management.
- ▶ Process activities include registration and deployment of software components and configuration changes.
- ▶ The actors that are involved in this control are IT operations roles, IT service support, and IT management roles.

## **Command and Control Management**

The Command and Control Management component has the following characteristics that relate to Security Operations:

- ▶ Ensure that all security processes and controls are working correctly.
- ▶ Process activities include following up on the dashboards that provide situational awareness about security posture in general, monitoring and analyzing security alerts, and triggering security incident processes if needed.
- ▶ The actors that are involved in this control are the actors in the CISO office.

## **Security Policy Management**

The Security Policy Management component has the following characteristics that relate to Security Operations:

- ▶ Monitor Security Policy Management-related activities.
- ▶ Process activities include monitoring policy deployment, verification of the version (is the correct version of the policy active), and collecting metrics about the enforcement of the policies to measure its effectiveness.
- ▶ The actors that are involved in this control are the CISO office and the operations personnel.

## **Software, System, and Service Assurance**

The Software, System, and Service Assurance component has the following characteristics that relate to Security Operations:

- ▶ Monitor Software, System, and Service Assurance-related activities.
- ▶ Process activities include monitoring the deployment of the applications, verifying that the endpoint agents are up and running, detection of unmanaged endpoints, and the verification of whether scheduled tests were run.
- ▶ The actors that are involved in this control are system administrators and application owners.

## **Data and Information Protection Management**

Data and Information Protection Management has the following characteristics that relate to Security Operations:

- ▶ Monitor all the technical controls that realize Data and Information Protection Management processes.
- ▶ Process activities include ensure that software agents are up and running, detection of unprotected data repositories, and monitoring correct execution of data disposal procedures.
- ▶ The actors that are involved in this control are the CISO office, data owners, database administrators, and security operations personnel.

As an example, the IT Service Management Foundational Security Management component and the corresponding operational support processes that are based on well-known process frameworks, such as ITIL or COBIT, are only a subset of the latter process frameworks. The different aspects of the Security Operations are shown in Figure 4-11 with two types of monitoring: monitoring the elements in the IT infrastructure, and monitoring the security operation processes.

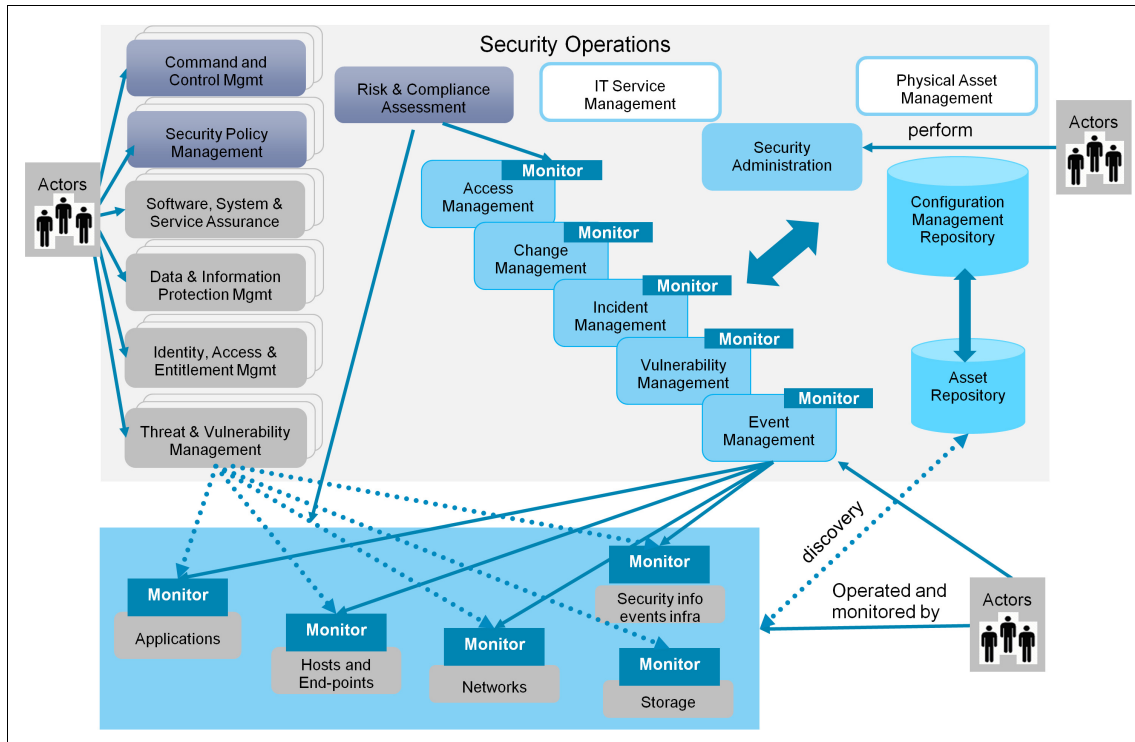


Figure 4-11 IT Service Management example

Security monitoring verifies the behavior of the infrastructure components (see the blue rectangle in Figure 4-11). The processes are monitored for their effectiveness (based on KPIs). The processes that are shown in Figure 4-11 are Access Management, Change Management, Incident Management, Vulnerability Management, and Event Management.

Operational support processes are equally important in the design of the security architecture. The O-ESA Security Operations, being an important part of the security architecture, address the following three key factors:

- ▶ People and partners
- ▶ Processes
- ▶ Tools and technologies

Although the tools and technologies are the focus of the Security Technology Architecture and are the easiest part, deploying security systems that address only one of the key factors (for example, tools or processes) are not going to achieve the wanted results. If operational support processes do not include tools to support the factors around how, when, and who use the processes, you run into a high probability of poor implementation and compliance.

The operational view of the security architecture addresses how people run, monitor, and manage your security services. A dedicated section in the architecture document should contain information about how the system is subject to support and operational requirements, particularly around how they are monitored, managed, and administered. It must be clear about how the architecture provides the ability for operation and support teams to monitor and manage the security services. How is this task achieved across all tiers of the architecture? How can operational staff diagnose problems? Where is the error information logged? Those are typical questions that must be addressed in the security architecture process.

## 4.4 Conclusion

This chapter has shown how the IBM Security Blueprint and the Open Enterprise Security Architecture can be combined to develop policy-driven security architectures. The IBM Security Blueprint can provide the foundation for a Security Management System, and O-ESA can complement it with a layered architectural approach, which is combined with the definition of the required security operations.

The capabilities of the IBM Security Blueprint can be translated to policy enforcement points in the infrastructure layer. The approach to create a security architecture can be used with a template to describe the security services that must be deployed in the organization.







## Business scenario for the Mobile Device Security solution pattern

This chapter introduces a typical business scenario of a fictional cardio healthcare company, referred to as *the cardio healthcare company* or the *company*. It shows how the company can use the IBM Security Framework and IBM Security Blueprint to help secure and facilitate their usage of mobile devices.

This chapter includes the following sections:

- ▶ Company overview
- ▶ Business vision
- ▶ Business requirements
- ▶ Security requirements
- ▶ Security architecture

## 5.1 Company overview

The cardio healthcare company is a healthcare provider that focuses on providing specialized cardiovascular-related healthcare services in the US. The company was founded in California and then expanded across the country. It operates stand-alone clinics in several states, where each clinic occupies its own building and provides preventive care and outpatient services. For surgery and other inpatient services, the cardio healthcare company uses operating environments in partner hospitals. The cardio healthcare company also participates in research programs.

The cardio healthcare company maintains financial and confidential health information about its customers (patients, research partners, and affiliated hospitals). All records are kept in electronic form. One of the key applications is the *Patient Web Portal*, where, by using a personal portal page, patients can access their personal health records, payment information, and so on. In addition, email communication is available between patients and service providers.

Another key application is the physician Healthcare Information System (Electronic Health/Medical Records), whereby using a personal portal page, physicians can access patient records, medication data, order examinations and tests, and have a limited view (subset) of patient records of other physicians.

Because the cardio healthcare company works closely with a few pharmaceutical companies on the latest drugs for heart disease, the exchange of confidential research-related information is extensive. Research information is also kept in an electronic form and shared over the network.

The cardio healthcare company has built a strong and long-term reputation and financial stability over the past 15 years in the US. The company's plan is to expand its operations within the US and to open healthcare centers in international markets.

The cardio healthcare company relies on two data centers: a *primary site* (in Phoenix, AZ) and a *backup site* (in Raleigh, NC). All production-related operations are performed in the primary data center. In terms of production, the backup data center is used for disaster recovery only.

The backup data center is also used for development and quality assurance (QA) tests on the applications and the infrastructure. Most of the business applications are web-based. All clinics are considered to have isolated internal networks that communicate with the production servers at the primary site. The endpoint systems in the intranet networks are primarily workstations that run Microsoft Windows. In addition, most of the clinic's modern healthcare appliances (such as electrocardiogram (ECG) and nuclear diagnostic imaging systems) are also connected to its network and generate patient-related data, which is considered part of a patient's data record.

Figure 5-1 shows the geographical distribution of the provider.

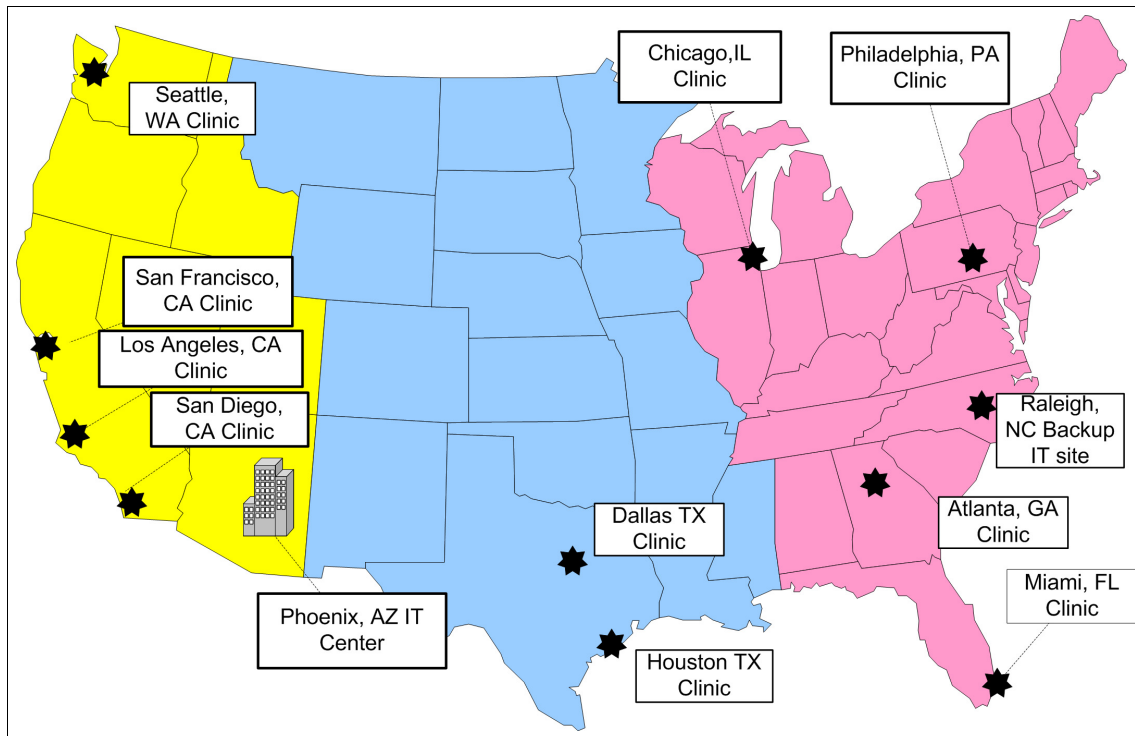


Figure 5-1 Geographical distribution of the cardio healthcare company

Section 5.5, “Security architecture” on page 191 provides more detailed information about the information technology (IT) infrastructure that supports this business.

## 5.2 Business vision

This section highlights the future direction that the cardio healthcare company plans to move its business development toward in the next five years:

- ▶ Expand business to the European Union (EU) by opening a clinic in Munich, Germany.

By collaborating with some pharmaceutical companies on research in the EU, the cardio healthcare company wants to expand its business that is related to heart diseases by opening a clinic in Europe. The project is scheduled to begin in two years, and the opening is planned in the next four years.

- ▶ Reduce costs by reusing the solutions and by using the lessons that are learned from the current IT infrastructure.

The cardio healthcare company wants to reuse its architectural and implementation approach wherever possible. While it copies the general infrastructure design, it tries to improve challenges found during operations and remediate them at an early phase.

- ▶ Respond to changing business needs and technology directions that can help improve customer experience by using new technologies.

Business goals are always reassessed and are constantly changing depending of the organization's needs. More often, the Internet is becoming a part of everyone's life. An increasing number of patients are using email as a communication tool with their doctors. In addition, patients are using the web applications for reviewing their own medical records and to manage appointments online.

Long term, the cardio healthcare company is looking to interconnect with other healthcare providers through the Smart Healthcare System. This system involves other aspects of health business, such as pharmaceutical and insurance.

The emergence of mobile technology brought about several changes within the company, including the introduction of updated policies that allow employees to use their own mobile devices to access company resources. Cardio healthcare company intends to expand this capability to patients that are visiting their facilities in the mid to long term.

The myriad of constant changes requires a greater flexibility in IT technology. However, new technologies and means of communication open the possibility for new threats and vulnerabilities.

- ▶ Manage the budget by avoiding penalties because of non-compliance with major regulations, such as HIPAA, SOX, and PCI-DSS.

In the healthcare industry, as in many others, non-compliance with regulations and standards can lead to significant financial fines and other types of penalties. The cardio healthcare company is successful in managing compliance with major regulations and is looking to maintain this preferred practice while they expand the business.

- ▶ Protect the company image and reputation by avoiding patient information leakage, preventing security attacks, and practicing security with due care and due diligence.

Any security intrusions, or leakage of any type of patient information (health, financial, or personal type), can lead to a loss of trust and damage to the reputation of the cardio healthcare company. The bottom line is that, besides losing money on penalties, it leads to a loss of customers and missed revenue opportunities. This aspect is particularly challenging with Bring Your Own Device (BYOD) mobile devices.

- ▶ Allow the business to grow and embrace new technology in a way that is safe and supports new business models, potentially enhancing performance and customer satisfaction with the new technology services offered by the business.

## 5.3 Business requirements

Based on the visionary aspects that are highlighted in 5.2, “Business vision” on page 180, the cardio healthcare company wants to achieve the following short-term business goals:

- ▶ Improve the quality and availability of patient care and satisfaction by delivering an excellent and individualized healthcare experience.
- ▶ Increase the protection of all patient-related information, and address the diverse security risks that are driven by compliance requirements, emerging technologies, data explosion, and so on.
- ▶ Embrace emerging technologies, such as mobile devices to enable physicians and patients around-the-clock access to company resources to enhance the patient care experience.
- ▶ Facilitate the management and demonstration of an overall compliance posture with data privacy laws and industry regulations, such as HIPAA and Payment Card Industry Data Security Standard (PCI-DSS).

Overall, the cardio healthcare company wants a mature security solution that can prevent information leaks, and provide trustworthy authentication methods and individual traceability and accountability of all actions that can impact a patient or patient records.

By addressing these pressing business requirements, the cardio healthcare company tries to achieve the following goals:

- ▶ Continue to manage an acceptable balance between preventing security risks and adversely affecting the business. User satisfaction levels are an important metric for IT projects at the cardio healthcare company.
- ▶ Constantly look for new and innovative solutions in all areas of the business, and always take security aspects into account.
- ▶ Be more proactive in security measures.
- ▶ Implement a robust and fit-for-purpose mobile device security solution that patients and physicians can use to access the necessary resources in a secure and consistent manner.
- ▶ Raise security awareness throughout the company by practicing corporate security education. Informed users are more likely to accept and support the security standards that are enforced.

### **5.3.1 IBM Security Framework mapping to business requirements**

Based on the following information, the IT management team from the cardio healthcare company can articulate their needs better to come up with a solution design:

- ▶ The IBM Security Framework definitions for business-driven security (described in 1.4, “IBM Security Framework” on page 8).
- ▶ The business requirements of the cardio healthcare company, which are described in 5.3, “Business requirements” on page 181.
- ▶ The current organizational infrastructure, which is described in 5.2, “Business vision” on page 180.

Through this scenario, the assigned IT architects can derive the functional requirements by using the underlying IBM Security Blueprint:

#### **▶ People**

The cardio healthcare company wants to use mature identity management and authentication processes and tools that help lower the costs that are related to this domain while it maintains their security standards and without putting undue stress on the user community.

The mobile device security solution that is designed for the cardio healthcare company in the following sections focuses on user and device authentication and authorization together with identity management in the People domain.

► Data

The cardio healthcare company uses a granular information asset classification scheme that is paired with a least privilege principle. Access to the Healthcare Information System (HIS) application and HIS database servers is strictly real-time monitored and enforced. There is a need to place governance around detecting sensitive data in-flight and monitoring the crossing egress points of the organization into mobile devices.

► Application

Application development focuses on the *secure by design* principle. The cardio healthcare company follows a rigorous release management process with a granular promotion-to-production path that specifies security testing criteria. This approach helps with practicing security during the application development phase and helps you discover any application vulnerabilities.

The processes of the cardio healthcare company achieved a high level of automation and embrace security controls, such as separation of duties and creation of auditable records.

► Infrastructure

The cardio healthcare company deployed network segregation. Systems are assigned to a security zone according to the sensitivity of the system and the data that is on it. The various security zones are separated by firewalls and intrusion prevention systems. Remote users must authenticate to a VPN server before they enter the network.

An area that must be focused on with the introduction of mobile devices is Network Access Control (NAC). This focus ensures that the mobile devices brought into the IT environment meet all of the requirements of the companies' security policies and that the mobile devices do not cause unnecessary exposure to the company by introducing malware and other threats to their IT environment.

The mobile device solution that is designed for the cardio healthcare company in the following sections focuses on security control configuration and management, the usage of NAC to control access to the network, and containerization on mobile devices to enable remote wipe of sensitive data if a device is lost or stolen.

Physical Infrastructure controls are also embraced in the security program of the cardio healthcare company. Respective controls for physical access controls to facilities and systems are also present in all locations. All systems that can access data of value (including personal data of patients) are either in closed office environments or in a secure virtual environment.

► Governance, Risk Management, and Compliance (GRC)

The cardio healthcare company practices strong compliance enforcement by managing a security controls framework and strict audit and security awareness program. Adequate audit reporting should always be delivered to satisfy auditors that are assessing the company's stance about important regulations for the operations of the cardio healthcare company in the healthcare industry.

The company realizes that more control is required, though, and wants to implement a robust control objective measurement and management solution that the company can use to configure, enforce, and manage controls on mobile devices that are introduced into the environment.

The mobile device solution that is designed for the cardio healthcare company in the following sections focuses on control objective measurement in the Governance, Risk Management, and Compliance domain.

Now, you take the next step in understanding the functional requirements and mapping them to the IBM Security Blueprint, followed by high-level look at the implementation approach.

## 5.4 Security requirements

To correctly address the new business requirements, the cardio healthcare company must enhance their mobile device security infrastructure. The cardio healthcare company defines the following high-level security requirements:

- To better manage its compliance posture with data privacy laws and industry regulations, the company must employ a cost-effective and centralized management solution for security configuration policies and audit data. It must also integrate the proposed new security solution to the existing incident and problem management solution.
- To better protect all patient-related information and to address the diverse security risks that are driven by, for example, eHealth initiatives, emerging technologies, and data explosion, the company must protect against information leakage. Such leakage might be because of intrusions and zero-day attacks. The company must also protect its critical servers with extra layers of intrusion prevention.



- ▶ To improve the quality and availability of patient care and satisfaction by delivering an excellent and individualized healthcare experience, and to increase caregiver productivity and reduce administrative costs, the company must address unavoidable delays in the IT change management processes. This requirement helps to improve the security posture of the servers of the company and of all nonstandard (embedded) operating systems of medical appliances that are connected to the network.

In addition to these distinct functional requirements, which are in line with the business requirements, the cardio healthcare company has more, valid functional requirements that require examination:

- ▶ Respond more in real time to intrusion detection and prevention (blocking) events.
- ▶ Detect and, if possible, automatically counteract detected attacks.
- ▶ Provide a solution that is more proactive to security threats.

The cardio healthcare company already uses some solutions to identify and eliminate security threats that enable attacks against systems, applications, and devices. However, the level of automation and the speed of these activities, in addition to the information available for Threat and Vulnerability Management, can be improved.

### **5.4.1 IBM Security Blueprint mapping to security requirements**

Now, you understand the security requirements for the extra security measures that the cardio healthcare company must implement. Yet you still must determine which specific solutions can potentially fulfill the security requirements. By using the IBM Security Blueprint, you can better explain and map the functional requirements into specific blueprint areas, and identify the appropriate solutions to implement within the IT environment of the company.

The overview of the components from the IBM Security Blueprint is shown in Figure 5-2 and Figure 5-3 on page 189.

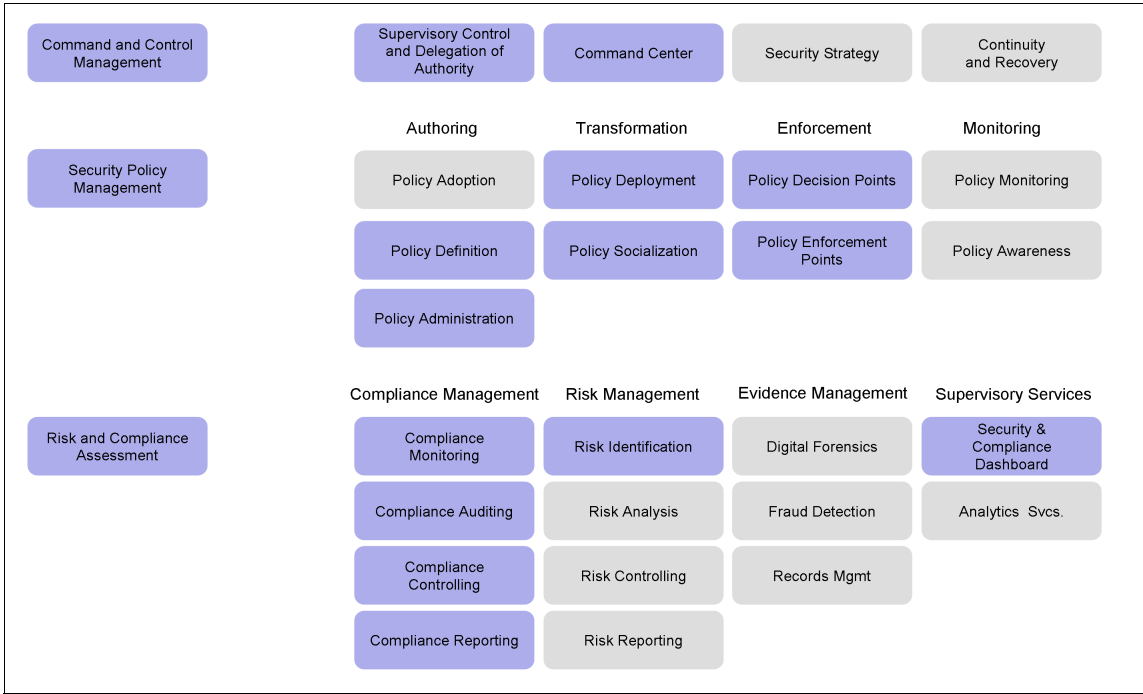


Figure 5-2 Foundational Security Management components for functional requirements

Let us start by taking a closer look at each of the IBM Security Blueprint subcomponents that are shown in Figure 5-2.

**Command and Control Management**

For this Foundational Security Management component, you must evaluate the following subcomponents:

- ▶ Security Control and Delegation of Authority  
Based on roles definition and governance policies, this subcomponent provides a segregated and access controlled solution to manage the overall IT environment, security policies, and report views.
- ▶ Command Center  
The Command Center provides a robust platform to support a centralized endpoint management solution for the entire organization.

## Security Policy Management

For this Foundational Security Management component, we must evaluate the following subcomponents.

- ▶ Policy Definition

Based on the current business requirements, the company must implement several security controls as soon as possible. For that task, the company uses a mature and market independent checklist as a guideline.

- ▶ Policy Administration

The Policy Administration subcomponent addresses the centralized endpoint lifecycle management of security administration policies, which include create, modify, delete, and other maintenance tasks for policies. Implement company-specific security controls, which are based on internal policies, to complete the security checklist requirements.

- ▶ Policy Deployment

This subcomponent provides a centralized architecture and a secure channel for security policy distribution and deployment to the mobile devices. The Policy Deployment is responsible for validating the deployment status, and in case of failure, it must redeploy the policies.

- ▶ Policy Socialization

In addition to defining specific policies that are enforced by security controls, this subcomponent ensures that employees, contractors, and anyone else that has direct access to the IT environment understands and adheres to the security policies for using mobile devices.

- ▶ Policy Decision Points

A Policy Decision Point analyzes the endpoint security posture and generates alerts about noncompliant configurations, which are based on the security policies that are already defined and applied for the IT environment.

- ▶ Policy Enforcement Points

Policy Enforcement Points enforce internal and external IT endpoint security controls. The standard security configuration, which reflects the organizational security policy, must be enforced on all mobile devices always. If changes occur on mobile devices, either accidentally or maliciously, the changes must be identified and the standard security configuration must be reapplied.

## **Risk and Compliance Assessment**

For this Foundational Security Management component, you must evaluate the following subcomponents.

- ▶ **Compliance Monitoring**  
Compliance Monitoring constantly checks security configuration reports to analyze and identify security threats and configuration management issues and deviations. It can provide real-time compliance reports, which are based on a security and compliance endpoint policy.
- ▶ **Compliance Auditing**  
Compliance Auditing provides a historical database to retain the audit data about endpoint-specific compliance posture and overall organization endpoint compliance statistics.
- ▶ **Compliance Controlling**  
Compliance Controlling provides different compliance views and compliance policy rules that are based on business requirements, such as country, type of machine, and organization department.
- ▶ **Compliance Reporting**  
This subcomponent provides compliance reports and audit information that is based on organizational security controls and federal standards preferred practices, including real-time and historical reports.
- ▶ **Risk Identification**  
Risk Identification refers to the ability to discover, recognize, and verify the existence of specific risks. It also encompasses the structuring of risk by mapping it into clearly defined classification schemes that can be specific to the industry or even to the risk taxonomy of an individual organization.
- ▶ **Security and Compliance Dashboard**  
A Security and Compliance Dashboard helps identify and report in real-time fashion the threats, compliance posture, and vulnerabilities that are found on the managed mobile devices, which are based on patches information, security configuration, and policies.

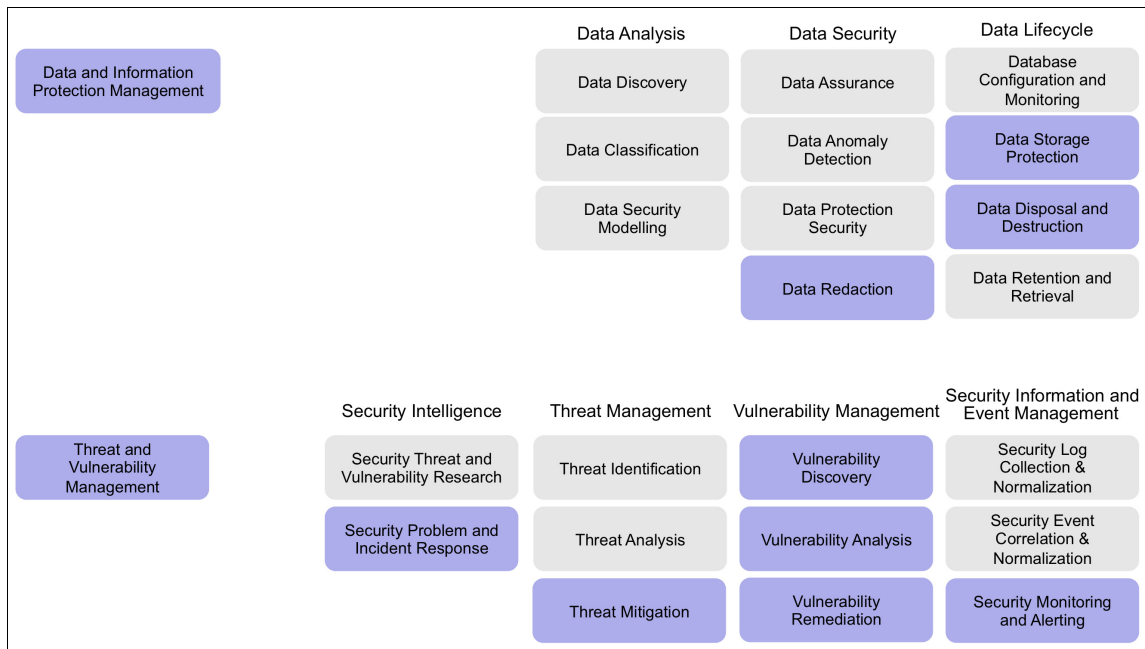


Figure 5-3 Foundational Security Management components for functional requirements

Let us take a closer look at each of the IBM Security Blueprint subcomponents that are shown in Figure 5-3.

## Data and Information Protection Management

For this Foundational Security Management component, you must evaluate the following subcomponents:

### ► Data Redaction

Data Redaction prevent sensitive and confidential data from being accessed and viewed on a mobile device that is based on the companies security policies. For example, a physician may be able to view confidential health information about a patient while he is in the hospital or his office, but not while he is accessing the patient information from other locations.

### ► Data Storage Protection

This subcomponent protects all of the sensitive and confidential data that is stored on a mobile device. The sensitive data should always be encrypted. If a mobile device is being used for both business and personal use, the business data should be maintained separately from personal data so that the business data can be remotely wiped without affecting the personal data when an employee leaves the company.

- ▶ Data Disposal/Destruction

This subcomponent remotely wipes all data from a mobile device when it is lost or stolen. If the device is owned by an employee, only the business data is remotely wiped when that person leaves the company.

## Threat and Vulnerability Management

For this Foundational Security Management component, you must evaluate the following subcomponents:

- ▶ Security Problem and Incident Response

Security Problem and Incident Response provides an analysis of identified attacks on mobile devices and recommendations on actions to take to resolve the security incident.

- ▶ Threat Mitigation

Threat Mitigation represents the implementation of real-time security reports for alerting you about security risks that are based on a noncompliant security configuration, either with internal security policies or external security regulations. Based on the integration with security alert bulletins sent by operating system and third-party application vendors, an automated patch installation process is triggered to correct the issues that caused the threat to the IT environment.

- ▶ Vulnerability Discovery

Vulnerability Discovery helps you identify the mobile devices with out of date patches, which are based on the published security bulletin information from operating system and third-party application vendors. Based on internal security policies or federal security configuration preferred practices, such as the *US Federal Desktop Configuration Control (FDCC)* or the *Defense Information Systems Agency Security Technical Implementation Guides (DISA STIGs)*, the mobile devices are assessed for a noncompliant security configuration.

- ▶ Vulnerability Analysis

The Vulnerability Analysis in this case is only responsible for reporting the vulnerability ratings, which are based on the federal agencies preferred practices analysis, such as FDCC and DISA STIGs.

- ▶ Vulnerability Remediation

Vulnerability Remediation mitigates security risk and threat exposures and improves IT services quality by implementing a patch management solution that ensures mobile devices are at the latest patch levels.

► Security Monitoring and Alerting

Security Monitoring and Alerting implements historical and real-time reports to consistently monitor the mobile device security behavior to validate deviations of standard operations in a period.

## 5.5 Security architecture

This section describes the architectural iterative steps that you can take to develop an enterprise security architecture from the IBM Security Blueprint. This section shows the approach that is outlined in the previous sections for the security architecture of the cardio healthcare company user scenario.

This approach includes a series of nine main activities, each of which breaks down into further subactivities, some of which are explained throughout the remainder of the section.

Here the top-level activities that are described in more detail in the following subsections:

1. Gather requirements.
2. Define strategy, planning, and policies from the requirements (program management and governance).
3. Define security domains (logical architecture).
4. Define security services placement in the security domains.
5. Define a component model for the security services (logical architecture).
6. Define use cases for the security services (logical architecture).
7. Define an operational model for the security services (physical architecture).
8. Define security operations for the concerned security services (security operations).
9. Validate the architecture and perform a risk assessment that is based on anomalous flows (risk management).

## 5.5.1 Gathering requirements

The security and privacy services to be incorporated within the Healthcare Information System and infrastructure must be based on firm business requirements. Business requirements (see 5.3, “Business requirements” on page 181), together with functional, non-functional requirements and security requirements, security use cases and user scenarios, and architecture concerns and constraints are common inputs to the security architecture. The requirements gathering activity typically consists of multiple subactivities: requirements identification and reuse, analysis, specification, and validation.

Table 5-1 provides a list of security requirements that were gathered for the Healthcare Information System and Infrastructure and were mapped against the Foundational Security Management components and security area. Each security requirement has an identification for tracing purposes.

*Table 5-1 Gathering security requirements*

Identifier	Requirement	Area	Foundational Security Management component
SR01	The HIS system shall ensure that only authenticated users can access its protected content.	Authentication	Identity, Access, and Entitlement Management
SR02	The system is required to have an access control mechanism that governs which data users can view, modify, and interact with.	Authorization	Identity, Access, and Entitlement Management
SR03	Actors of the system should be identified by a unique user identification (name or number).	Identification	Identity, Access, and Entitlement Management
SR04	<ul style="list-style-type: none"><li>► Detect and, if possible, automatically counteract detected attacks.</li><li>► Provide a solution that is more proactive to security threats.</li></ul>	Threat protection	Threat and Vulnerability Management
SR05	All patients health information must be safeguarded from unauthorized disclosure.	Integrity	<ul style="list-style-type: none"><li>► Software, System, and Service Assurance</li><li>► Data and Information Protection Management</li></ul>



Identifier	Requirement	Area	Foundational Security Management component
SR06	Respond more in real time to intrusion detection and prevention (blocking) events.	Intrusion detection	<ul style="list-style-type: none"> <li>▶ Threat and Vulnerability Management</li> <li>▶ Risk and Compliance Assessment</li> </ul>
SR07	All modifications to sensitive data must be electronically signed.	Non-repudiation	<ul style="list-style-type: none"> <li>▶ Software, System, and Service Assurance</li> <li>▶ Data and Information Protection Management</li> </ul>
SR08	Protection against data leakage.	Privacy	<ul style="list-style-type: none"> <li>▶ Software, System, and Service Assurance</li> <li>▶ Data and Information Protection Management</li> <li>▶ Risk and Compliance Assessment</li> </ul>
SR09	Centralized management solution for security configuration policies and audit data.	Security auditing	<ul style="list-style-type: none"> <li>▶ Command and Control Management</li> <li>▶ Risk and Compliance Assessment</li> </ul>
SR10	Auditing should meet regulatory requirements.	Compliance	Risk and Compliance Assessment
SR11	To continue to function in the event of an unforeseen interruption (primary data center failure), recovery takes place at the backup data center. The target to recover the primary data center is within one day.	Business continuity	<ul style="list-style-type: none"> <li>▶ IT Service Management</li> <li>▶ Command and Control Management</li> <li>▶ Security Policy Management</li> </ul>
SR12	Physical devices should be protected against destruction, damage, theft, and tampering.	Physical protection	<ul style="list-style-type: none"> <li>▶ Physical Asset Management</li> <li>▶ Security Policy Management</li> </ul>

Identifier	Requirement	Area	Foundational Security Management component
SR13	Unavoidable delays in the IT change management processes.	System Maintenance Security	IT Service Management
SR14	Mobile devices should be protected against security threats and malware. Only secured and endpoint managed mobile devices can access to corporate data.	Mobile device security	<ul style="list-style-type: none"> <li>▶ Physical Asset Management</li> <li>▶ Software, System, and Service Assurance</li> </ul>

## Cardio Healthcare Company user scenario

The following user scenario is used as input to the security architecture.

Physicians use their company owned mobile devices (tablet PCs and notebooks) from different locations (clinic, partner hospitals, university, and home) to access different types of information (operations schedules, research information services at an affiliated university, and sensitive patient data) while they operate in different roles. The physicians entitlement to IT resources depends on which context the clinician is operating in. Access to sensitive patient data should be granted only when the physician is acting as a specialist (surgeon), and not when he is acting as a researcher. Access can also depend on the physician's location (hospital or partner hospital) or the type of device (tablet, PC, or notebook).

The hospital maintains confidential health information about its customers (patients, research partners, and affiliated hospitals). All patient records are kept in electronic form. One of the key applications is the physician healthcare information system (Electronic Health/Medical Records), where, by using a personal portal page, physicians can access patient records, medication data, ordering examinations and tests, and have a limited view (subset) of patient records when they are acting as a consulting physician. A primary physician can see all of the fields in the medical records of his patient. When a record is used by another physician to ask for an opinion, information such as medical history are important, but the consulting physician does not need to refer to the SSN, phone number, or address.

Because the hospital works closely with affiliated universities on the latest development of new techniques in cardiac surgery, the exchange of confidential information is extensive. Research information is also kept in an electronic form and shared over the network.

The system context model provides a view of the system's boundaries and how the system interacts with other external organizations. It helps identify some key architectural artifacts that are required to build the complete solution. The information flow between the system and each external system provides key inputs to the information model.

Figure 5-4 shows an overview of this use case scenario.

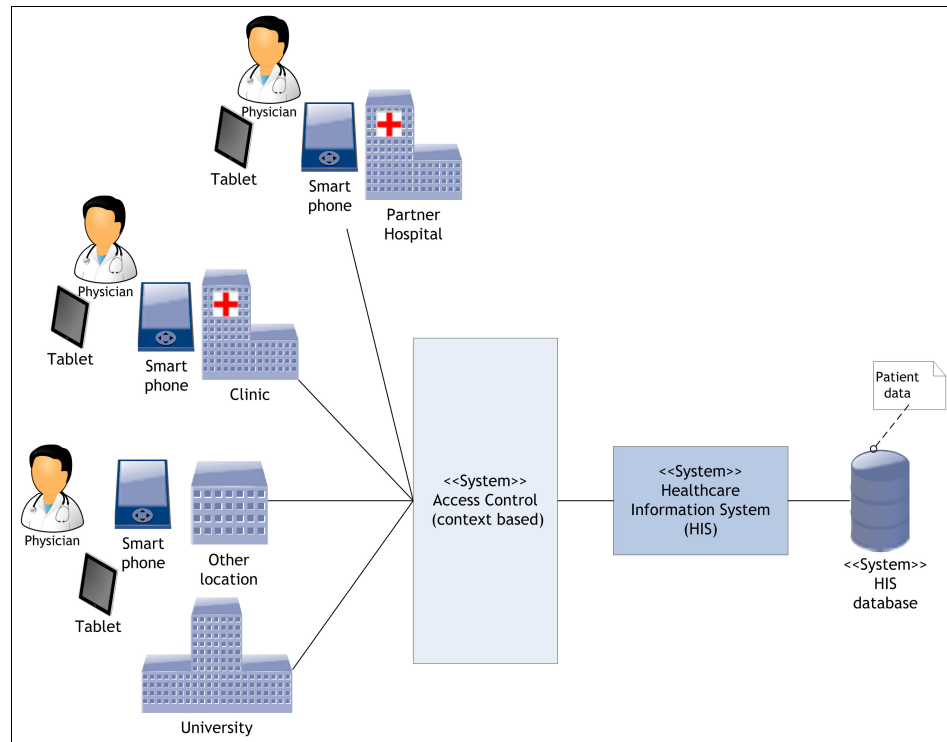


Figure 5-4 Context diagram for the Healthcare Information System

### 5.5.2 Defining strategy, planning, and policies from the requirements (program management and governance)

Part of the step to derive policies from requirements is the understanding of the existing security controls of the current environment and privacy regulations. Security controls include the mechanisms that are used by hardware and software systems, networks, databases, personnel, and applications, which are critical to the business. Privacy regulations have an impact on the treatment of information.

The review of existing security controls should follow these sections of ISO/IEC 27002:

1. Information Security Policy
2. Organization of Information Security
3. Assets Management
4. Human Resources Security
5. Physical and Environmental Security
6. Communications and Operations Management
7. Access Control
8. Information Systems Acquisition, Development, and Maintenance
9. Information Security Incident Management
10. Business Continuity Management
11. Compliance

To fulfill the requirements of the cardio healthcare company user scenario, the following policies are identified (see Figure 5-5 on page 197):

- ▶ Information security policy (chain of trust partner policy and mobile devices security policy)
- ▶ Access control policy (password use and unattended user equipment)
- ▶ Human resources security (termination or change of employment and return of assets)
- ▶ Compliance policy (with legal and security policies)
- ▶ Operations management policy
- ▶ Asset management policy (responsibility for assets and information classification)
- ▶ Business continuity management policy
- ▶ Physical and Environmental Security (equipment maintenance and disposal)
- ▶ Information Systems Acquisition and Development and Maintenance (technical vulnerability management)

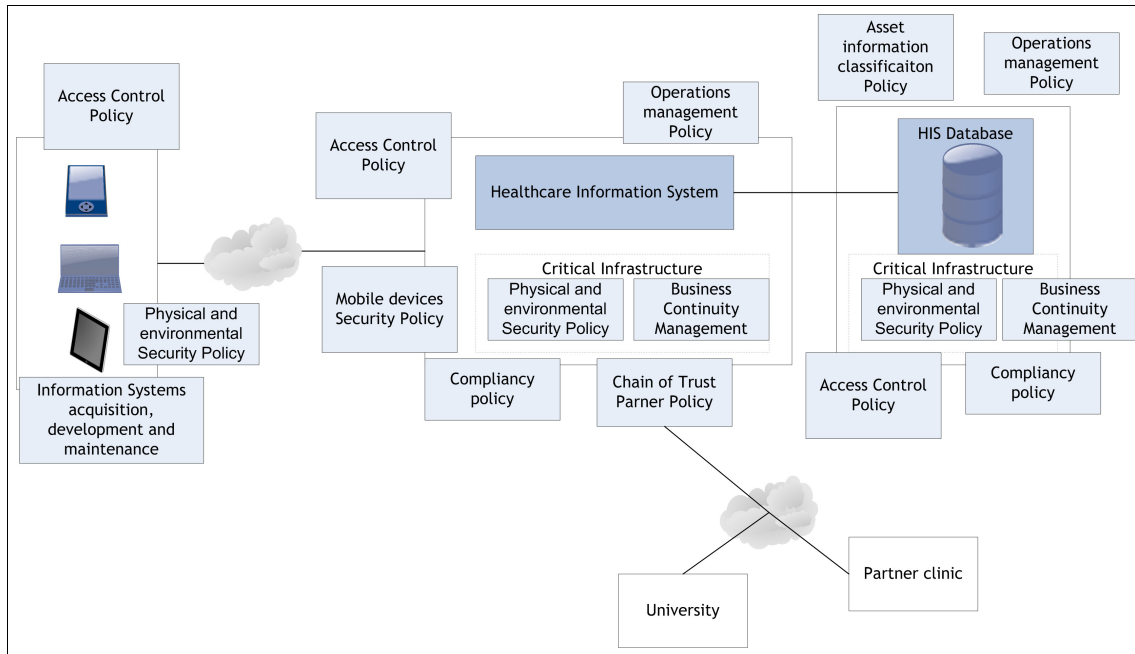


Figure 5-5 Identification of the security policies that are derived from the requirements

### 5.5.3 Defining security domains (logical architecture)

Security zoning is an element of the design of a security architecture, which segments information assets (data, business applications, system management, and hardware) into a logical grouping with the same security requirements and policies. Zoning restricts access and data flows to components, and the components are separated by perimeters (containing the network interfaces and control flow of data).

The cardio healthcare company user scenario logical architecture addresses the following security zones:

<b>Uncontrolled</b>	Refers to anything outside the control of an organization. Access from the uncontrolled environment to systems in the controlled zone could be through many channels.
<b>Controlled</b>	Restricts access between uncontrolled and restricted (a traditional DMZ).
<b>Restricted</b>	Access is restricted and controlled. Only authorized individuals gain entrance and there is no direct communication with external sources (Internet).

<b>Secured</b>	Access is available only to a small group of highly trusted users. Access to one secured area does not necessarily give access to another.
<b>External controlled</b>	An external zone in which data is stored by business partners external to the systems where there is limited trust in the protection of data (for example, credit reporting agencies, banks, and government agencies).

Figure 5-6 shows an overview of these security zones.

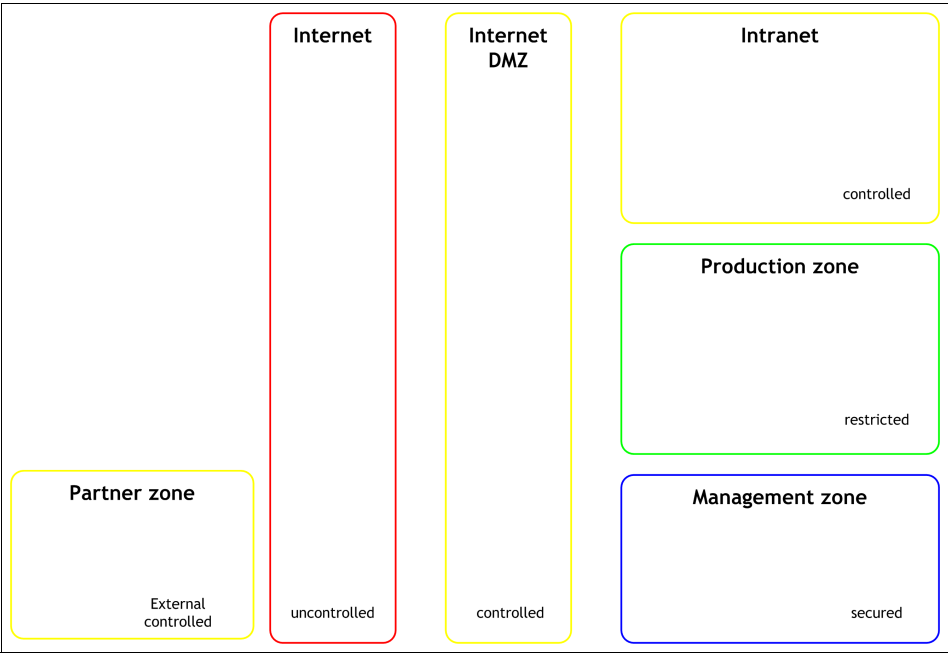


Figure 5-6 Network zones in the cardio healthcare company

### 5.5.4 Defining security services placement in the security domains

A security service is a logical construct that represents a set of functional requirements in an architecture. After you derive the security zones that are involved in the architecture, your next step is the appropriate placement of security services in the identified zones. A security service can be accessed from other zones than the zone in which it is. A Security Service Description Form (see Table 4-1 on page 159) can be used to describe the different attributes, scope, and functionality of the required security services.

Table 5-2 represents some examples of the security services that are required per network security zone.

*Table 5-2 Security services that are required per network security zone*

Security Service Name	Services to provide	Foundational Security Management component	Zone
Intrusion detection	A security service to stop threats from impacting network assets.	<ul style="list-style-type: none"> <li>▶ Threat and Vulnerability Management</li> <li>▶ Security Policy Management</li> <li>▶ Risk and Compliance Assessment</li> </ul>	Internet DMZ zone
Endpoint protection	A security service that addresses the protection of mobile devices.	<ul style="list-style-type: none"> <li>▶ Threat and Vulnerability Management</li> <li>▶ Security Policy Management</li> <li>▶ Risk and Compliance Assessment</li> </ul>	Internet zone
Security administration	A security service that provides a central point for the administration of security devices.	Physical Asset Management	Management zone
Identity Federation SSO	A security service that provides identity relationships and mapping to transform identities across trust domains.	Identity, Access, and Entitlement Management	Production zone

In policy driven security services, the splitting of enforcement and decision point allows for the reuse of the decision point by multiple enforcement points. This split promotes component reuse across the architecture. Enforcement points can be tightly integrated with the decision point (for example, a firewall) or loosely coupled (for example, an XML firewall). An example of tight coupling is a network security service where policies enforce a set of rules for network traffic, identifying which traffic can pass through the service. The decision point takes the necessary actions on the traffic that passes. An example of a loosely coupled enforcement and decision point is a web service authentication service (for example, XML firewall) that is coupled with an authorization service in another zone.

Figure 5-7 shows the security services that are mapped to the different zones for the cardio healthcare company user scenario and the enforcement points.

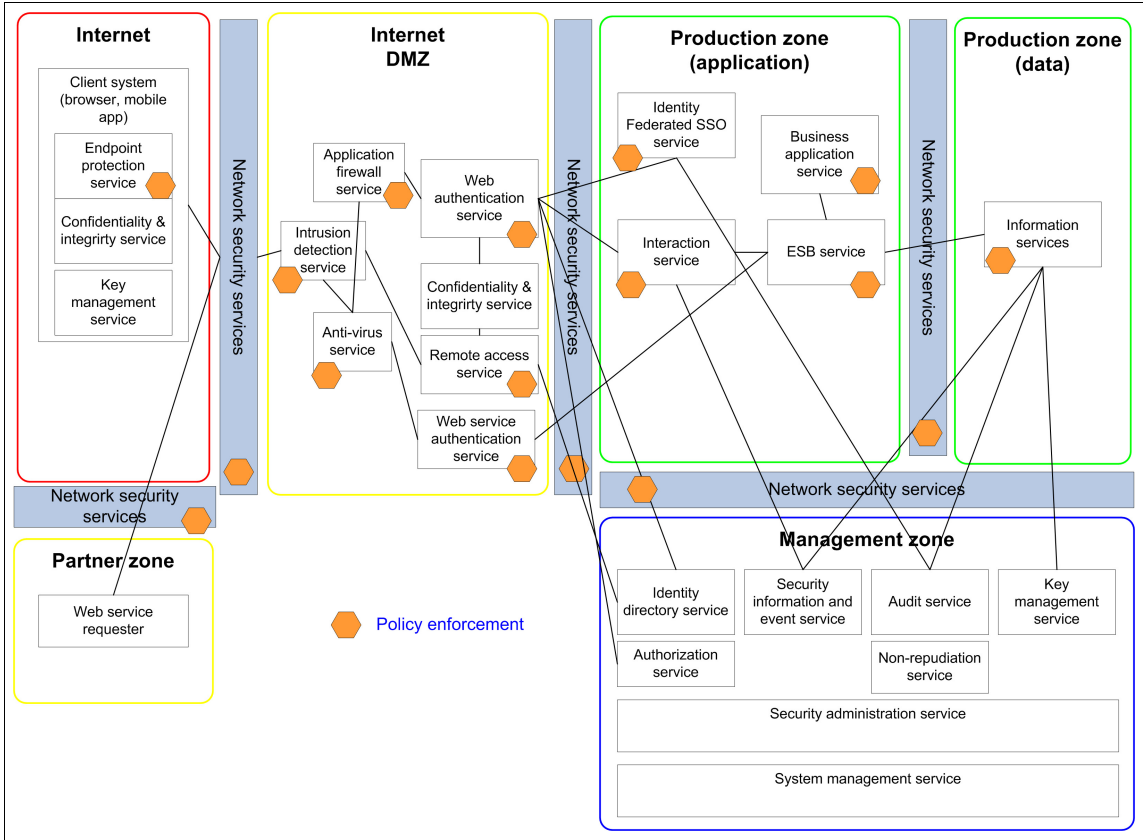


Figure 5-7 Security services placement for the cardio healthcare company user scenario



## 5.5.5 Defining a component model for the security services (logical architecture)

The component model, which is shown in Figure 5-8, identifies the core elements that are required to provide the service, which is defined in 5.5.4, “Defining security services placement in the security domains” on page 198. As part of the scope of the cardio healthcare company scenario, the component model captures the solution outline for some of the alternative authentication and authorization options. The component model is a logical representation of the architecture and must be viewed with the operational model to establish how the solution is delivered.

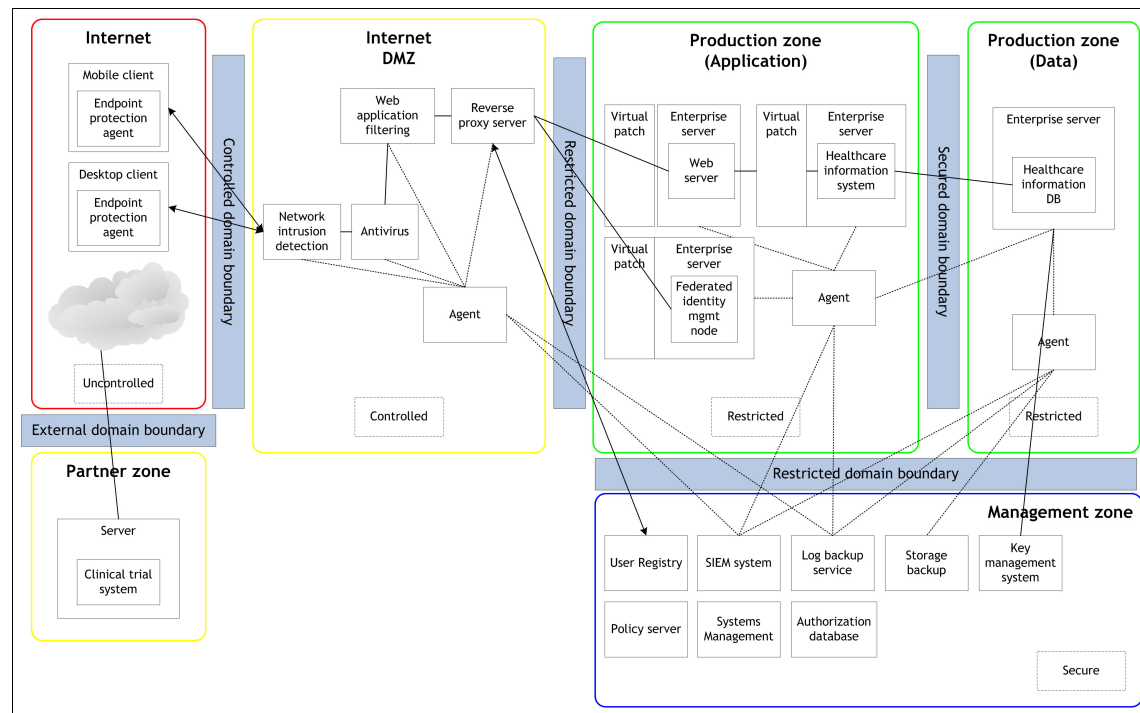


Figure 5-8 Component model for the security services of the cardio healthcare company user scenario

## 5.5.6 Use case

In this activity, the most common use cases for the concerned security services of the architecture are documented. This section provides an example of a use case for controlled access to the Healthcare Information System through a tablet PC (controlled access use case).

Table 5-3 and Table 5-4 provide an overview of the human and non-human actors.

*Table 5-3 Human actors*

Human actors	Short description of the actor
Physician	Any person with the role of Surgeon who has a cardio healthcare company account and can log in to the healthcare company information system.
Hacker	A person that is committed to the circumvention of the security of the mobile devices that are used by employees or the security of the cardio healthcare company systems.

*Table 5-4 Non-human actors*

Non-human actors	Short description of the actor
Authentication and authorization service	The system that is responsible for the validation of identity for access control purposes. The system allows or denies access to resources based on a set of policies.
Policy service	The system that is responsible for defining, translating, and distributing policies.
Anti-virus service	A software system to detect, prevent, and remove malicious software, and to protect against threats from viruses.
Healthcare Information System	An information portal system that is used by physicians that provides patient records, medication data, and a process for ordering examinations and tests.

An example of controlled access use cases is described in Table 5-5.

*Table 5-5 Controlled access use cases*

<b>Scope &amp; level</b>	A physician is visiting the protected portal page of the Healthcare Information System with his tablet PC through a secured communication channel.
<b>Goal in context</b>	An actor is accessing the protected portal hosted on the cardio Healthcare Information Portal.
<b>Preconditions</b>	The actor has a valid account, company card ID, and password, and the necessary permissions (through an ACL) to access the protected portal page. The actor has the role of primary physician.
<b>Successful outcome</b>	The actor (primary physician) has access to a protected portal page that contains patient data after authentication.

	<b>Failure</b>	<b>Outcome</b>	<b>Condition leading to outcome</b>
<b>Failure Outcomes</b>	Invalid password message	No access to protected portal page	Wrong password
	Invalid credential message	No access to protected portal page	Wrong account
	Invalid credential message	No access to protected portal page	Wrong Company CARD ID
<b>Primary actor</b>	Primary physician		
<b>Secondary actors</b>	<p>Through a link on the cardio healthcare company portal page:</p> <ol style="list-style-type: none"> <li>1. An actor uses a company owned mobile device with the necessary endpoint protection.</li> <li>2. An actor has a secured remote connection to the cardio healthcare company network.</li> <li>3. An actor opens a link to the cardio healthcare company portal. The actor clicks a Healthcare Information System (HIS) link.</li> <li>4. The system displays the login page.</li> <li>5. An actor provides a valid account, card ID, and password, and submits the page.</li> </ol> <p>The system determines the security context, which is based on the authenticated user, to the system, the location of access to the network, the user agent of the device, IP address, time, the primary physician relationships, and other information, and shows a portal page that contains information that corresponds to the determined security context.</p>		
<b>Main scenario</b>	Through a secured link on the cardio healthcare company portal.		
<b>Alternatives</b>			
<b>Variations</b>	A protected portal link through the partner hospital information portal.		
<b>Related information</b>			
<b>Issues</b>			

The use case is also shown in Figure 5-9.

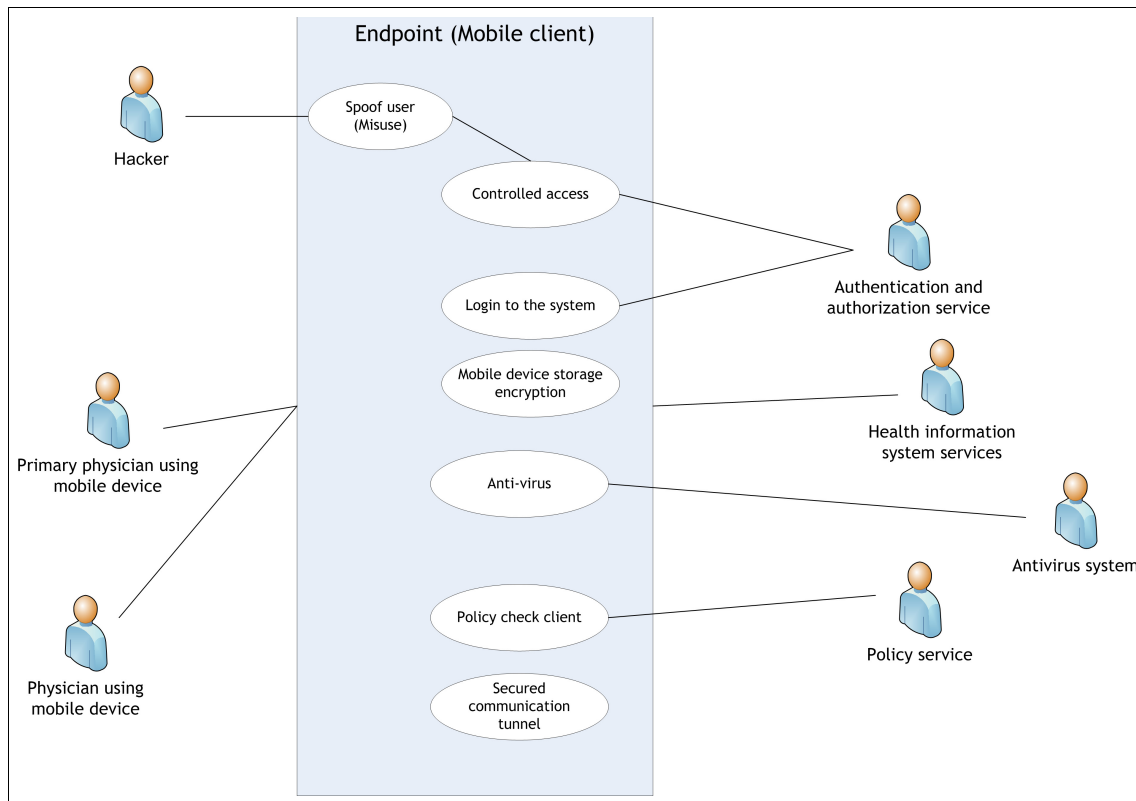


Figure 5-9 Use case model for the cardio healthcare company user scenario

## 5.5.7 Operational model

The operational model of the enterprise security architecture is a representation of a network of systems, associated peripheral devices, systems software, middleware, and application software. The operational model can include one or more diagrams that show the topology and geographic distribution of the system and network connections and where and how users and external systems interact with the security systems.

A detailed design activity can handle more technical aspects of quality properties (redundancy, availability, and disaster recovery protocols). The operational model for the cardio healthcare company user scenario restricts the level of detail to the node level that contains one or more components that are deployed on the node.

Web Security Servers (reverse web proxies) are in the Internet DMZ to manage access to the applications from the Internet. The Web Security Servers help consolidate access management for the external users who are accessing web applications. The Web Security Servers perform centralized authentication and authorization before it allows access to the web applications. All existing network infrastructure components (such as firewalls, switches, and routers) are designed and implemented in an HA (redundancy) configuration.

Application servers and database servers are in separate network zones and are isolated from each other by using firewalls.

The IT standards of the cardio healthcare company require all servers to use a UNIX or Linux technology-based operating system that has the following configuration:

- ▶ Application and database servers operate on UNIX.
- ▶ Web Security Servers operate on Linux.
- ▶ The secure File Transfer Protocol (SFTP) server operates on Linux.
- ▶ Domain name servers (DNSes) and email servers operate on Linux.
- ▶ The server components that are deployed in the Management Zone operate on UNIX.

Centralized access control management is implemented. All web-based access is controlled by using Web Security Servers. In addition, operating system-level access is enforced on critical servers that use local security agents. The following critical servers are identified:

- ▶ The secure FTP server (Linux) that contains confidential research reports.
- ▶ Application and database servers in the Production Zone (UNIX).

Centralized log collection, analysis, and reporting on compliance for the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS), Sarbanes-Oxley Act (SOX), and ISO/IEC 27002:2005 is enforced by using Security Information and Event Management (SIEM) technology. This technology integrates the Web Security Server infrastructure. It also offers operating system-level monitoring that can collect logs from critical UNIX, Linux, and Windows servers. The SIEM solution is also able to monitor the network traffic flows between the components for abnormalities (unusual behavior) and identify data structures that are moving across the wire.

A distributed database real-time monitoring system is implemented by using Database Activity Monitoring technology. This system monitors all database activities in real time, including privileged user access, without the performance impact and separation-of-duties issues of native database logging. This solution also provides capabilities, such as blocking, workflow management, and vulnerability assessments for the databases. The solution is also monitored from the enterprise SIEM dashboard. The resulting compliance reports are able to include all enterprise database events from the DAM system.

Figure 5-10 shows an operation model of the IT infrastructure of the cardio healthcare company by using the network zone representation.

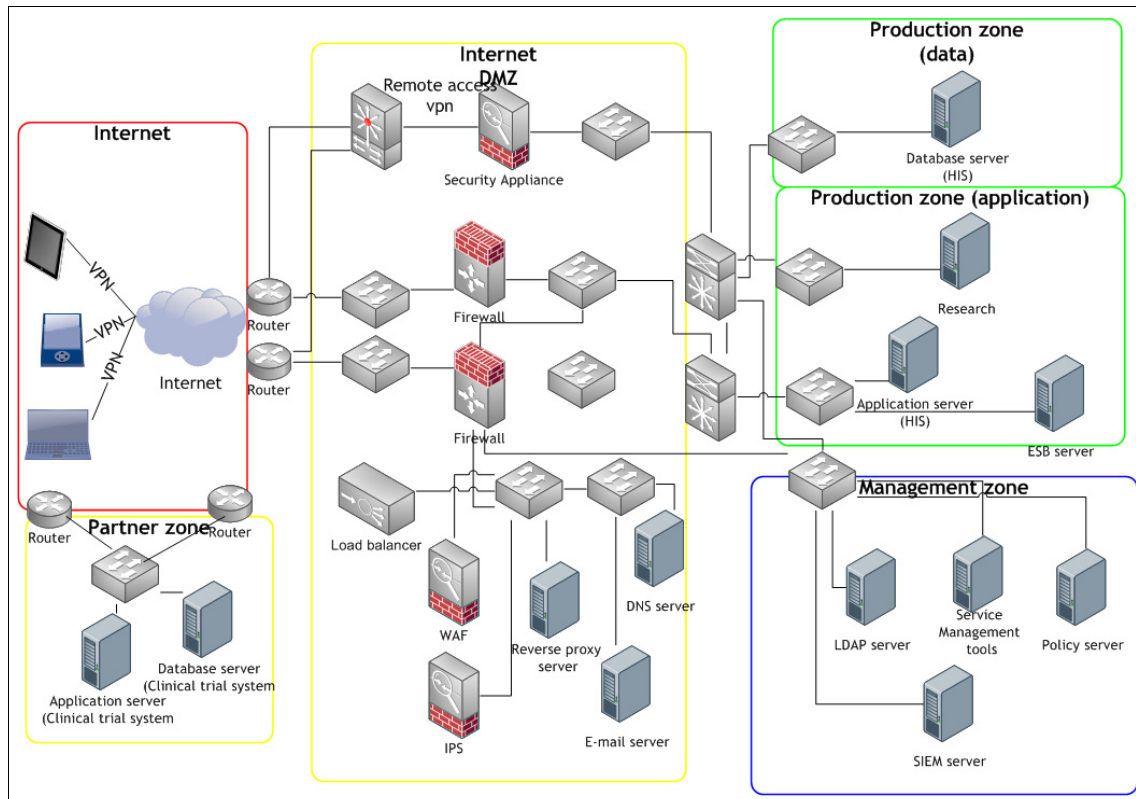


Figure 5-10 Operational model

### **5.5.8 Defining security operations for the concerned security services**

After they deploy the security services on the nodes within the enterprise, the IT operations of the security service must ensure that the configuration and operation are correct. The security services must be monitored against failure, and the security service must be reliable and available within the agreed service levels. This task is within the domain of IT Service Management. IT Service Management encompasses all the activities that are required to operate the security services. The following list shows some examples of activities that are provided by IT Service Management:

- ▶ Monitoring compliance to enterprise security standards
- ▶ Active and proactive reaction to security threats
- ▶ Proactive and reactive monitoring of security services failure, analyzing the root cause, and restoration.
- ▶ Analysis, control, and reporting of the performance of security services to ensure sufficient capacity.

You can use IT asset management to maintain an inventory of the assets that are deployed in the enterprise. IT asset management is tightly linked to IT Service Management activities.

Figure 5-11 shows an operational view of the SIEM services of the cardio healthcare company, which are linked to IT Service and Asset Management.

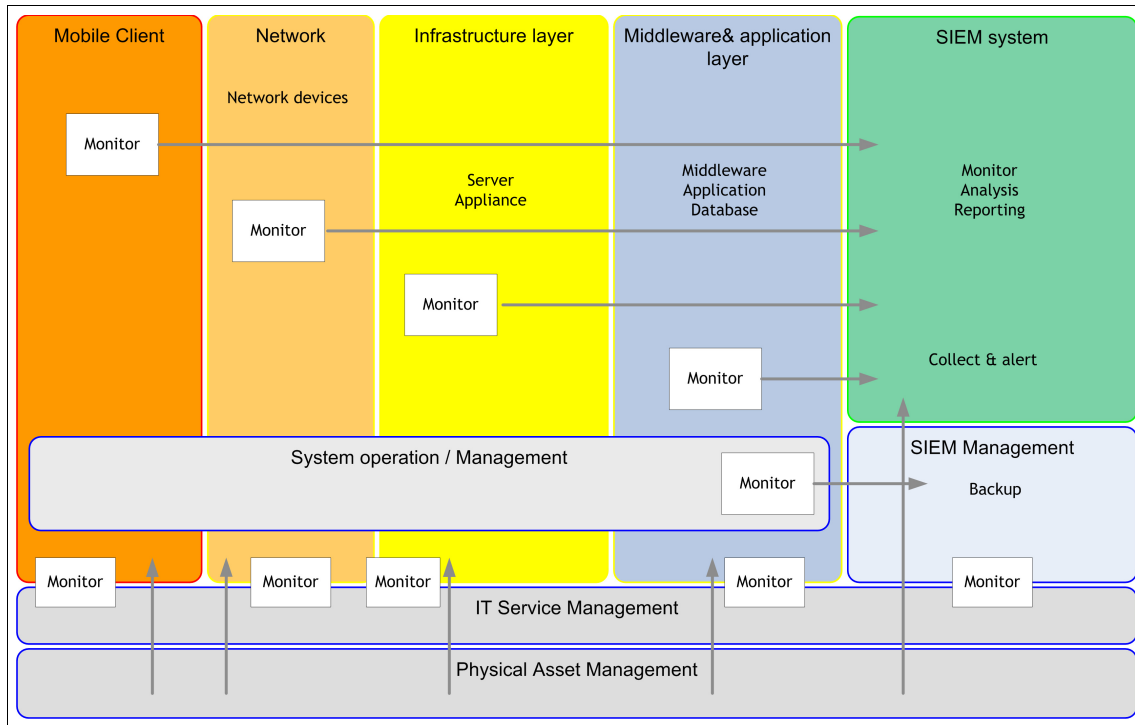


Figure 5-11 Operational view of the SIEM service

## 5.6 Conclusion

By combining the IBM Security Blueprint and Open Enterprise Security Architecture, you can start from business requirements and evolve to an operational model.

In this chapter, the IBM Security Blueprint was used to identify the necessary components and their corresponding capabilities. This chapter applied the steps that are described in Chapter 4, “Using O-ESA to develop an enterprise security architecture” on page 145 to this specific case. The security capabilities were translated into placements of Policy Enforcement Points that are distributed throughout the infrastructure, and we showed how security operations can be set up.



This chapter depicts a hands-on use case of the IBM Security Blueprint, and it can be used to develop a security solution design. The IBM Security Blueprint can be used in many other ways as well, depending on the context and the needs of the organization.



# Related publications

The publications that are listed in this section are considered suitable for a more detailed discussion of the topics that are covered in this book.

## IBM Redbooks

The following IBM Redbooks publications provide more information about the topic in this document. Some publications referenced in this list might be available in softcopy only.

- ▶ *Enterprise Security Architecture Using IBM Tivoli Security Solutions*, SG24-6014
- ▶ *IBM Security Solutions Architecture for Network, Server and Endpoint*, SG24-7581
- ▶ *Security in Development: The IBM Secure Engineering Framework*, REDP-4641

You can search for, view, download, or order these documents and other Redbooks, Redpapers, Web Docs, draft and additional materials, at the following website:

[ibm.com/redbooks](http://ibm.com/redbooks)

## Other publications

These publications are also relevant as further information sources:

- ▶ *Enterprise Security Architecture: A Business-Driven Approach*, Sherwood, et al, CRC Press, 2005, ISBN 157820318X
- ▶ *Open Enterprise Security Architecture (O-ESA)*, Van Haren, Van Haren Publishing, 2011, ISBN 9087536720

## Online resources

These websites are also relevant as further information sources:

- Payment Card Industry Data Security Standard

The Payment Card Industry Data Security Standard (PCI DSS) was developed and is governed by the PCI Security Standards Council, which consists of the five major payment brands. The PCI DSS is a multifaceted security standard, and its objectives are to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. The PCI DSS security standard provides a baseline of technical and operational requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures that are designed to protect cardholder data. PCI DSS applies to all entities involved in payment card processing, including merchants, processors, acquirers, issuers, and service providers, and all other entities that store, process, or transmit cardholder data. PCI DSS is composed of a minimum set of requirements for protecting cardholder data, and may be enhanced by extra controls and practices to further mitigate risks.

<https://www.pcisecuritystandards.org>

- Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act (GLBA) was enacted in 1999 by the United States of America Congress. The GLBA covers banks, savings and loans, credit unions, insurance companies, and securities firms. It even includes some retailers and automobile dealers that collect and share personal information about consumers to whom they extend or arrange credit. The GLBA provides a set of security and privacy rules for the affiliation of banks, securities firms, and other financial services that regulate the collection and disclosure of private financial information, and stipulates that financial institutions must implement security programs to protect such information and the pretesting provisions, which prohibit the practice of pretesting accessing private information and ensure the security and confidentiality of customer information.

<http://business.ftc.gov/privacy-and-security/gramm-leach-bliley-act>

► Federal Information Processing Standard

The Federal Information Processing Standards (FIPS) are a series of information technology security and privacy standards that describe the cryptographic processing, encryption algorithms, and other information technology standards. The intended audience is non-military government agencies and contractors who work with the agencies within the United States of America. It assures that an overall implementation provides an acceptable level of security.

<http://www.itl.nist.gov/fipspubs/>

► Bank for International Settlements (Basel III)

The Basel Committee on Banking Supervision is a committee of banking supervisory authorities that was established with the objective to enhance the understanding of supervisory issues and improve the quality of banking supervision worldwide. It seeks to do so by exchanging information about national supervisory issues, approaches, and techniques, with a view to promoting common understanding. The committee uses this common understanding to develop guidelines and supervisory standards in areas where they are considered wanted. In this regard, the committee is best known for its international standards on capital adequacy, the core principles for effective banking supervision, and the guidelines on cross-border banking supervision. The Basel III International framework for liquidity risk measurement, standards, and monitoring presents the Basel Committee's reforms to strengthen global capital and liquidity rules with the goal of promoting a more resilient banking sector. Basel III is built on the three pillars of the Basel II framework. The reforms raise both the quality and quantity of the regulatory capital base and enhance the risk coverage of the capital framework. They are underpinned by a leverage ratio that serves as a backstop to the risk-based capital measures. The Basel framework provides an extra layer of protection against model risk and measurement error, which includes the requirements for banks to perform their own internal assessments of externally rated securitization exposures, which are associated with credit risk mitigation practices.

<http://www.bis.org>

► Sarbanes-Oxley

The Sarbanes-Oxley (SOX) Act came into force in July 2002 and introduced major changes to the regulation of corporate governance and financial practice. It is named after Senator Paul Sarbanes and Representative Michael Oxley of the US legislative branch, who were its main architects.

The Sarbanes-Oxley Act sets a number of non-negotiable deadlines for compliance that are arranged into 11 titles. As far as compliance is concerned, the most important sections within these 11 titles are considered to be 302, 401, 404, 409, 802, and 906. Titles 302 and 404 are considered most important from the IT governance and IT security perspective, as they relate to the daily and annual financial reporting.

<http://www.soxlaw.com>

- European Union Data Protection Directive (EUDPD)

The European Union Data Protection Directive (EUDPD) was enacted in 1995 by the European Parliament and the Council of the European Union covering the protection of personal data and the free movement of such data within the EU. Under EU law, personal data can be gathered legally only under strict conditions. For legitimate purposes, a person or organization must protect personal data from misuse and respect certain rights of the data owners. Specific rules for the transfer of personal data outside the EU must be followed to ensure the best possible protection under the EU privacy and human rights law.

[http://ec.europa.eu/justice/data-protection/index\\_en.htm](http://ec.europa.eu/justice/data-protection/index_en.htm)

- Department of Defense Architecture Framework

The Department of Defense Architecture Framework (DoDAF) was developed and is governed by the United States Department of Defense. The DoDAF provides a structure for a specific stakeholder concern through viewpoints that are organized by various views. It is an overarching, comprehensive architecture framework and conceptual model that enables the development of architectures to facilitate the ability of Department of Defense (DoD) managers at all levels to make key decisions more effectively through organized information sharing across the department, Joint Capability Areas (JCAs), mission, component, and program boundaries.

<http://dodcio.defense.gov/dodaf20.aspx>

- Family Educational Rights and Privacy Act

The Family Educational Rights and Privacy Act (FERPA) was enacted in 1974 by the US Department of Education. FERPA is a federal law that protects the privacy of student education records. Students have specific, protected rights regarding the release of such records. FERPA requires that an educational agency or institution ensures that any record that contains personally identifiable information that is directly related to the student is an educational record that is protected under FERPA.

<http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>

► National Institute of Standards and Technology

The US Department of Commerce's National Institute of Standards and Technology (NIST) is responsible for developing technical, management, physical, and administrative standards and guidelines to US industry, science, and the public. The NIST has a specific security research focus to identify emerging technologies and conceive new security solutions that can have a high impact on critical information infrastructures. The NIST also performs research on behalf of the US Department of Commerce. NIST looks into the early stages of technology development, develops proof of concepts, and references and transfers new technologies to all industry sectors. With this approach, they create and refine new standards, test methodologies, and assurance methods, including security, digital forensics tools and methods, access control and authorization mechanisms, Internet Protocol security, intrusion detection systems, quantum information system security and cryptography, and vulnerability analysis.

<http://www.nist.gov/index.html>

► Health Insurance Portability and Accountability Act

To improve the efficiency and effectiveness of the healthcare system, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, included Administrative Simplification provisions that required the US Department of Health and Human Services (HHS) to adopt national standards for electronic healthcare transactions and code sets, unique health identifiers, and security. At the same time, the US Congress recognized that advances in electronic technology could erode the privacy of health information. So, Congress incorporated provisions into HIPAA that mandated the adoption of federal privacy protections for individually identifiable health information.

HHS published a Privacy Rule in December 2000, which was later modified in August 2002. This rule set national standards for the protection of individually identifiable health information by three types of covered entities: health plans, healthcare clearinghouses, and healthcare providers who conduct the standard healthcare transactions electronically. Compliance with the Privacy Rule was required as of April 14, 2003 (April 14, 2004 for small health plans).

HHS published another Security Rule in February 2003. This rule sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information. Compliance with the Security Rule was required as of April 20, 2005 (April 20, 2006 for small health plans).

<http://www.hhs.gov/ocr/privacy/>

► Information Technology Infrastructure Library

Information is the most important strategic resource that any organization must manage. Key to the collection, analysis, production, and distribution of information within an organization is the quality of the Information Communication Technology (ICT) systems and IT services that are provided to the business. You must recognize that ICT systems are crucial, strategic, and organizational assets, so organizations must invest the appropriate levels of resources into the support, delivery, and management of these critical IT services and the ICT systems that underpin them. However, these aspects of IT are often overlooked or only superficially addressed within many organizations.

The Information Technology Infrastructure Library (ITIL) consists of modules that contain advice and guidance on the preferred practices that relate to the provision of IT services. ITIL is used as the basis for the development of a British Standard for Service Management. The standard and ITIL are aligned and the standard itself was recently revised and is now documented in the following set of documents:

- BS 15000-1:2002, IT Service Management  
(Part 1: Specification for Service Management)
- BS 15000-2:2003, IT Service Management  
(Part 2: Code of Practice for IT Service Management)

<http://www.itil-officialsite.com>

## Help from IBM

IBM Support and downloads

[ibm.com/support](http://ibm.com/support)

IBM Global Services

[ibm.com/services](http://ibm.com/services)





Using the IBM Security Framework and IBM Security Blueprint

(0.2" spine)  
0.17" <-> 0.473"  
90 <-> 249 pages







# Using the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security



**Building a business security reference model based on standards and common practices**

**Connecting business drivers with IT security and risk management**

**Explaining the value in a real world business scenario**

Security is a major consideration in the way that business and information technology systems are designed, built, operated, and managed. The need to be able to integrate security into those systems and the discussions with business functions and operations exists more than ever.

This IBM Redbooks publication explores concerns that characterize security requirements of, and threats to, business and information technology (IT) systems. This book identifies many business drivers that illustrate these concerns, including managing risk and cost, and compliance to business policies and external regulations. This book shows how these drivers can be translated into capabilities and security needs that can be represented in frameworks, such as the IBM Security Blueprint, to better enable enterprise security.

To help organizations with their security challenges, IBM created a bridge to address the communication gap between the business and technical perspectives of security to enable simplification of thought and process. The IBM Security Framework can help you translate the business view, and the IBM Security Blueprint describes the technology landscape view. Together, they can help bring together the experiences that we gained from working with many clients to build a comprehensive view of security capabilities and needs.

This book is intended to be a valuable resource for business leaders, security officers, and consultants who want to understand and implement enterprise security by considering a set of core security capabilities and services.

## INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

### BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

**For more information:**  
[ibm.com/redbooks](http://ibm.com/redbooks)