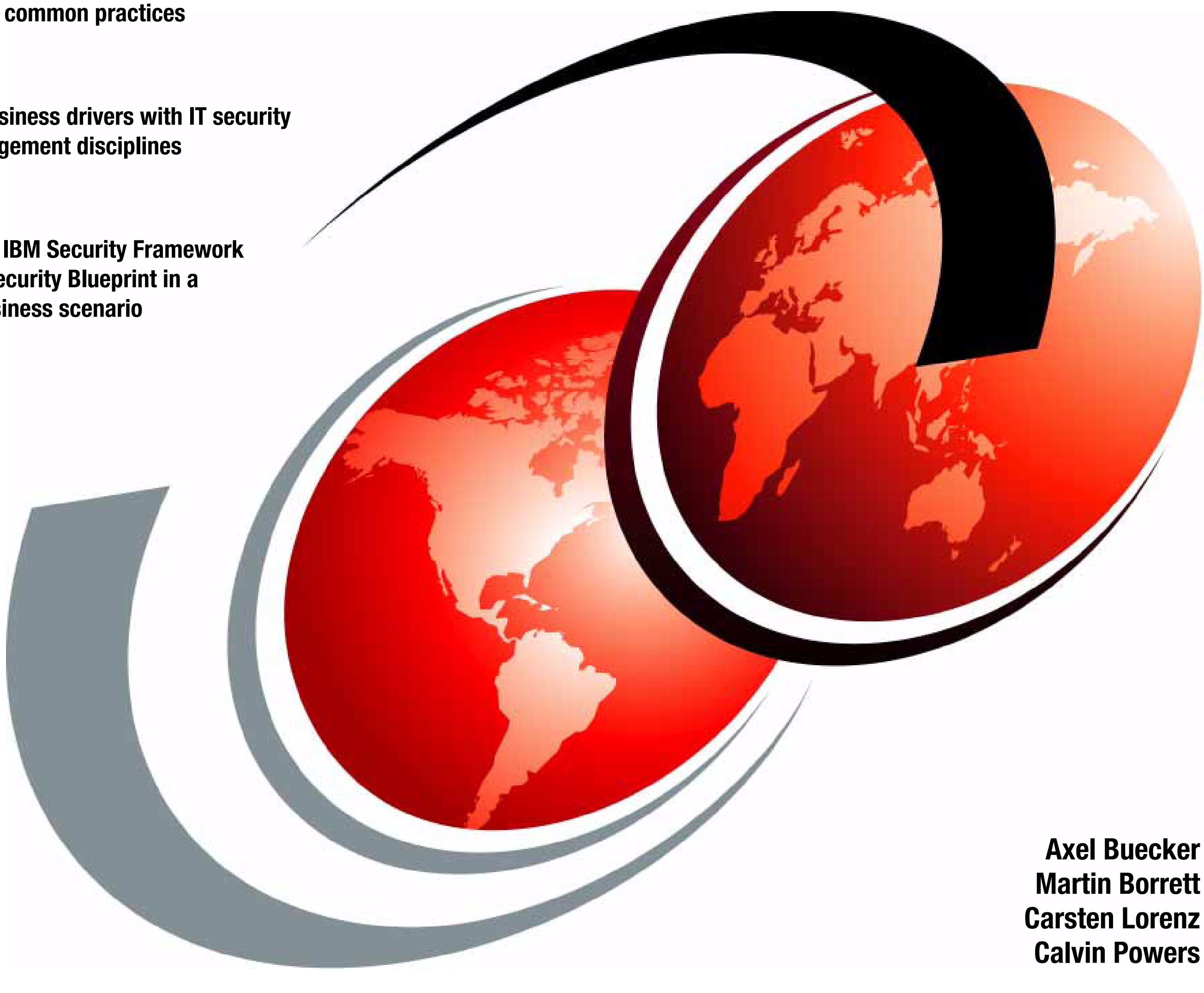
Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security

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

Connecting business drivers with IT security and risk management disciplines

Employing the IBM Security Framework and the IBM Security Blueprint in a real-world business scenario



Axel Buecker
Martin Borrett
Carsten Lorenz
Calvin Powers

Redpaper

ibm.com/redbooks

International Technical Support Organization

Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security

December 2010

REDP-4528-01

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

Second Edition (December 2010)

Contents

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 give 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 Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites 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.

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.

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®
Redbooks®
Redpaper™
Redbooks (logo) ®
Smarter Planet™

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

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

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 discussions with business functions and operations exists more than ever.

In this IBM® Redpaper™ publication, we explore concerns that characterize security requirements of, and threats to, business and information technology (IT) systems. We identify a number of the business drivers that illustrate these concerns, including managing risk and cost, and compliance to business policies and external regulations, showing how they can be translated into frameworks to enable enterprise security.

Over the last few decades, industry groups and standards bodies have developed frameworks that serve as a baseline for certain aspects of security, and in this IBM Redpaper publication we discuss two such frameworks:

- CoBiT
- ISO27002

To help you with your security challenges, IBM has created a bridge to address the communication gap between the business and the 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 solution view.

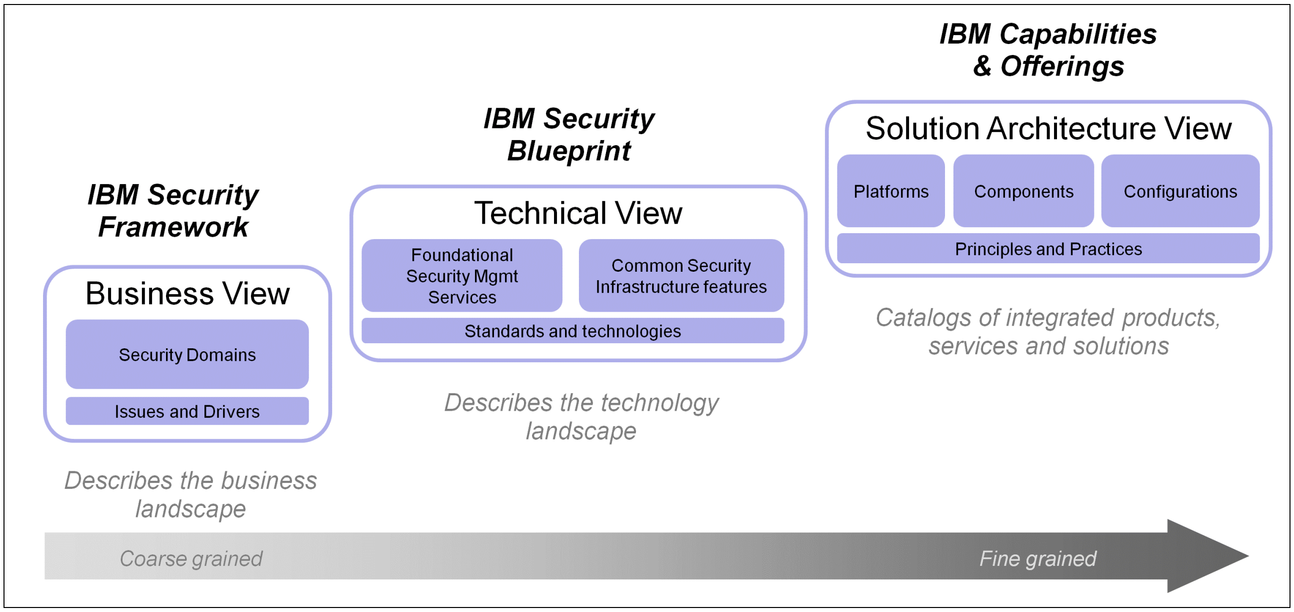

IBM Capabilities & Offerings
IBM Security Blueprint
IBM Security Framework
Solution Architecture View
Platforms
Components
Configurations
Principles and Practices
Technical View
Foundational Security Mgmt Services
Common Security Infrastructure features
Standards and technologies
Business View
Security Domains
Issues and Drivers
Catalogs of integrated products, services and solutions
Describes the technology landscape
Describes the business landscape
Coarse grained
Fine grained

Figure 1 Positioning the IBM Security Framework and IBM Security Blueprint

The IBM Security Framework divides Information Security into the following security domains:

- People and Identity
- Data and Information
- Application and Process
- Network, Server and Endpoint

- Physical Infrastructure
- Security Governance, Risk Management and Compliance

The IBM Security Blueprint expands on this business-oriented view of the IBM Security Framework by mapping the domains to a core set of security components representing capabilities and services. The IBM Security Blueprint aims to describe these security capabilities in vendor and product agnostic terms, using common, accepted industry definitions.

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

The team who wrote this paper

This was produced by a team of specialists from around the world working at the International Technical Support Organization (ITSO).

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 23 years of experience in a variety of areas related to workstation and systems management, network computing, and e-business solutions. Before joining the ITSO in March 2000, Axel worked for IBM in Germany as a Senior IT Specialist in Software Security Architecture.

Martin Borrett is the Lead Security Architect for IBM across Northern Europe. He advises at the most senior level clients on the business, technical, and architectural issues associated with security. Martin is a co-author of the IBM Redbooks® publication *Understanding SOA Security*, SG24-7310. He is Chairman of the IBM Europe Customer Security Forum and Vice Chairman of the IBM UK Technical Consulting Group. He is a member of the IBM Academy of Technology, a Fellow of the BCS, and a Chartered Engineer (CEng) and member of the IET.

Carsten Lorenz is a certified Senior Managing Consultant at IBM in the UK. He manages security solutions in large and complex IT infrastructure outsourcing engagements for customers throughout Europe, the Middle East, and Africa. He has more than 10 years of experience in the security and compliance field, specializing in the areas of security management, IT risk assessment, governance, and operational risk management. Carsten has performed consulting engagements with IBM customers in various industries, ranging from fortune 500 to SMBs. Carsten is a CISSP, CISM, and CISA, and he holds a bachelor's degree in European Studies from University of Wolverhamption, UK, and a diploma in Business Science from University of Trier, Germany.

Calvin Powers is a Technology Project Manager in the IBM Security Strategy Team. His current focus is on applying IT security technologies to the IBM Smarter Planet™ initiative and on research projects for the IBM Institute for Advanced Security. He is a member of the IBM risk management community and has a special interest in risk management methods applied to IT environments. Previously, he worked on privacy management, public key infrastructure, and network security projects in IBM.

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

David Crowther, Foulques de Valence, Guilherme Monteiro, Michel Oosterhof, Andrew Quap, Maria Schuett, Kai Stockmann

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

Nick Coleman, Stefaan van Daele, 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

Comments welcome

Your comments are important to us!

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

- Use the online **Contact us** review Redbooks form found at:

  ibm.com/redbooks

- Send your comments in an email to:

  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

1

Introducing the IBM Security Framework and IBM Security Blueprint

To set the scene for the IBM Security Framework and IBM Security Blueprint, we start with a discussion of the typical business context when it comes to information technology (IT) security and how business leaders can leverage security, risk, and compliance related investments to competitively position their organization and satisfy complex regulatory guidelines. We describe two existing frameworks:

- CoBiT
- ISO27002

The remainder of this chapter is dedicated to introducing the IBM Security Framework and the IBM Security Blueprint.

1.1 Business context for IT security

Organizations rely on computing systems and automation more than ever to detect threats to intellectual property, reputation, and privacy. These 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 the pace of globalization continues, traditional boundaries between organizations continue to disappear. The ideal response involves a level of planning and assessment to identify risks across key business areas, including people, processes, data, and technology throughout the entire business continuum. It is important to plan a holistic approach that can facilitate a business-driven security blueprint and strategy that can act as an effective shield of defense for the entire organization.

We believe that organizations have to build services that are *secure by design*, meaning that security is intrinsic to their business processes, their product development, and their daily operations. It is factored into the initial design, not bolted on afterwards. This allows an organization to securely and safely adopt new forms of technology, like cloud computing or virtualization, and business models like tele-working and outsourcing can be more safely leveraged for cost benefit, innovation, and shorter time to market.

With the security domains, capabilities, and services as a backdrop, this first section covers a detailed overview of the IBM Security Framework and IBM Security Blueprint. In the later sections we explain the IBM Security Blueprint in more detail by discussing its components and subcomponents. Later we take a closer look at the business context for areas such as identity management. We then look at the IBM Security Framework mapping and use the IBM Security Blueprint components and subcomponents and how they map to the needs of this scenario.

1.2 Drivers that influence security

Most of today’s projects are driven by both business and IT drivers, although we can probably agree that business drivers are almost always the initiating factor. Let us take a closer look at these influencing factors:

- Business drivers: Business drivers measure value, risk, and economic costs that influence their 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.
- 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.

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 in an organization.

IT drivers represent technical considerations that affect the trustworthiness of the IT environment and likely 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 values 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 proper 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. It 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 is a condition 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 might be tangible or intangible. For an e-retailer, these are tangible assets. For a financial services company, the asset might be the client information or other data used in transactions of the system.

Protection of the business asset value or brand image

This driver captures the firm's desire to protect its image. The loss of good will from a security incident or attack has a direct consequence to the business. Therefore, the security measures are likely to be proportional to the consequence. When the desire to avoid negative publicity increases, upon encountering a security breach, the stipulation for this driver becomes stronger.

Legal and regulatory compliance

Legal and regulatory compliance refers to the externally imposed conditions on the transactions in the business system and the company. This includes the rules and policies imposed by regulatory and government agencies. Civil, criminal liability, or regulatory penalty from a security incident or attack has a negative consequence on the business. Therefore, the amount of regulation and steps to ensure compliance should be factored in this driver. This includes privacy issues, the ability to prove the transaction initiator, and proving compliance.

Contractual obligation

Security measures for an IT system are likely to be proportional to the consequences encountered when the business encounters contractual liability from a security attack. Depending on the structure and terms of the contract, the consequence might lead to financial loss or liability. For example, when security incidents are encountered, 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 asset, theft of service, or fraud. Indirect loss might include loss based on civil or criminal judgment, loss of good will, or re-prioritized 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, transportation systems, computing, and so on. The loss of critical infrastructure by its provider might have a ripple effect, causing secondary losses and driving security decisions for those 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 system, life support, or other high-impact or time-dependent process.

1.2.2 IT drivers that influence security

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

Internal threats and threat agents

Security-related failures and incidents are caused by threats or threat agents found within the physical and logical boundaries of the organization or enterprise that operates and controls the IT system. These threats and threat agents 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. An example of a internal threat agent is a person who would use his ability to access the IT system or influence business or management processes to carry out a malicious activity.

External threats and threat agents

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

Examples of external threats are single points of failure for one or more business or management processes that are outside the enterprise boundary, such as a power system grid or a network connection, or a computer virus or worm that penetrates the physical or logical network boundary. An example of an external threat agent is a hacker, or someone who has 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 to meet its metrics for managing itself can be viewed as a security exposure to both business or management processes.

  An example of security exposure for service delivery is when IT operations processes cannot respond to critical events in a timely manner. Another is when IT resilience processes 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 will be 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 for our system 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, is a complex IT environment.

Business environment complexity

Because most businesses rely on IT, most business environments are an interconnected set of businesses, each with its own complex IT environment, business processes, and IT management processes. This complexity might contribute to the security or insecurity of the IT system.

Audit and traceability

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

IT vulnerabilities: Configuration

Configuration vulnerabilities are potentially present in every IT system, providing an opening to a potential attack based on the system and how it is designed and set up.

IT vulnerabilities: Flaws

Software flaws potentially exist in every IT system. These flaws represent vulnerabilities that were not detected and are not evident in the design documents. As such, they are an unexpected deviation from what was designed. An example is a defect in an operating system or application that is discovered after implementation.

IT vulnerabilities: Exploits

The basic design of software in any IT system might be exploited by threats or threat agents as a part of an attack on the IT system, the business, or the management processes. This might include the use of a function within a system in a way to compromise the system or underlying data. While certain people might define an exploit as both the flaw and the method, we treat them separately because an exploit might involve using normal functions as designed in an unusual manner to attack the system. The exploits can also be viewed as the openings or avenues that an attacker can use.

1.3 Common industry approaches to IT security management

IT security management is the term 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 reasons depicted in 1.2.1, “Business drivers that influence security” on page 3 are leading to an evolving number of enterprises that adopt internationally accepted frameworks and best practices to help implement IT governance in their enterprise. Control Objectives for Information and related Technology[1] (CobiT), the International Organization for Standardization 27002:2005[2] (ISO/IEC 27002:2005), and the Information Technology Infrastructure Library[3] (ITIL) have emerged worldwide as the most respected frameworks for IT governance and compliance. We take a closer look at CobiT and ISO/IEC 27002:2005 in the following sections because they have—in contrast to ITIL, which is more focussed on IT service management elements—a strong focus on IT security.

1.3.1 Control objectives for information and related technology

CobiT is a set of best practices (framework) for IT management created by the Information Systems, Audit and Control Association (ISACA) and the IT Governance Institute (ITGI) in 1996. It is an internationally accepted framework for IT governance and control. The current edition, 4.1, issued by the IT Governance Institute in 2007, includes the following sections:

- Executive summary (explains CobiT key concepts and principle)
- CobiT framework (explains the CobiT approach)
- Control objectives (defines a generic set of control requirements that need to be managed for each IT process to get effective control)
- Management guidelines (explains tools to measure, compare, and improve the performance of IT processes)

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

[2] 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.

[3] For more information about ITIL®, got to http://www.itil-officialsite.com/home/home.asp.

- 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 enterprise needs to support its business decisions. Business information itself is again 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, confidentially, integrity, availability, reliability, and compliance). CobiT defines 34 high-level processes that are grouped into the following four domains:

1. Plan and organize.

   This domain focuses on IT strategy: How can IT contribute to business objectives?
2. Acquire and implement.

   The topic of this domain is the identification, development, or acquisition and integration of IT solutions to realize IT strategy.
3. Deliver and support.

   This domain is about delivering and supporting the entire range of IT services.
4. 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 implementing CobiT, because business objectives must be clearly defined before the IT strategies can be aligned.

1.3.2 ISO/IEC 27002:2005

The British Standard 7799[4] that preceded the International Organization for Standardization 27002:2005 (ISO/IEC 27002:2005) is the most widely recognized security standard in the world. The last major publication was in May 1999, an edition that included many enhancements and improvements over previous versions. When 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 a significant number of control requirements, some extremely complex. Compliance with ISO/IEC 27002:2005 is, consequently, a far from trivial task, even for the most security conscious of organizations.

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 needed for ISO/IEC 27002:2005 compliance. From here, planning and implementing must be rigidly undertaken.

[4] Information about RiskServer, Security Risk Analysis, ISO17799, Information Security Policies, and Audit and Business Continuity can be found at http://www.riskserver.co.uk/.

ISO/IEC 27002:2005 contains 11 categories that have to be considered when applying an overall enterprise security approach. The categories are:

- 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

Now it is time for us to introduce the IBM Security Framework, which focuses on the *what*, not the *how.* It can help you translate your requirements into coarse-grained business solutions, not into specific IT components or IT services.

1.4 IBM Security Framework

Today's business leaders are expected to manage risk in their areas of responsibility in the same way that CFOs manage risks in their domains. Security risks and the potential impact on IT need to be communicated to executive peers in business terms. Additionally, they need to align IT security controls with their business processes, monitor and quantify IT risk in business terms, and dynamically drive business-level insight at the executive level. They need to manage risk and orchestrate security operations in a way that enforces compliance and optimizes business results.

As an organization secures its business processes, a business-driven approach needs to become the guiding influence for ensuring that all the different security domains work together in a holistic and synergistic manner, in alignment with the overarching business objectives. Otherwise, the organization's risk stance becomes vulnerable due to misalignment of priorities between IT and the business strategy. Using a standards-based approach to map business drivers to IT security domains is often difficult and is often an afterthought.

IBM created a comprehensive IT security framework (Figure 1-1) that can help ensure that every necessary IT security domain is properly addressed when using a holistic approach to business-driven security.

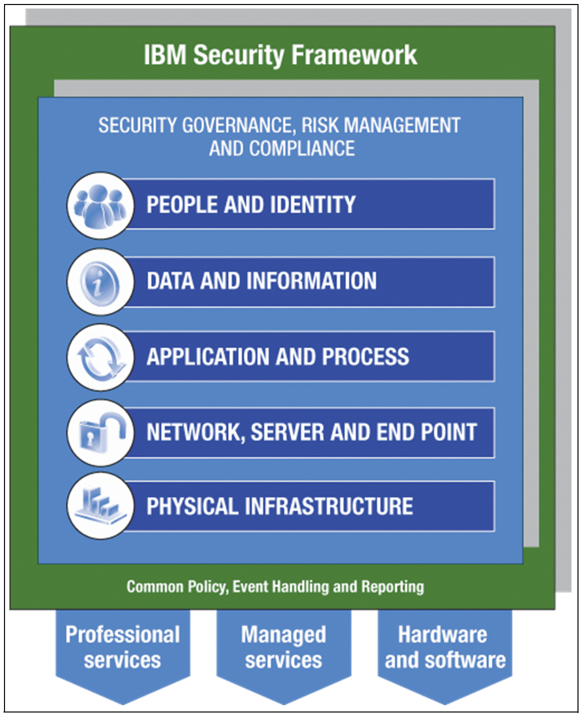


Figure 1-1 The IBM Security Framework

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.

Comprehensive professional services, managed services, and hardware and software offerings are available from IBM to support your efforts in addressing the following security domains covered by the IBM Security Framework.

1.4.1 Security Governance, Risk Management and Compliance

Every organization needs to define and communicate the principles and policies that guide the business strategy and business operation. In addition, every organization must evaluate its business and operational risks, and develop an enterprise security plan to serve as a benchmark for the execution and validation of the security management activities that are appropriate for their organization.

These principles and policies, the enterprise security plan, and the surrounding quality improvement process represent the enterprise Security Governance, Risk Management and Compliance model. Specifically, the requirements and the compliance criteria for the remaining security domains are:

- People and Identity

  This domain covers aspects about how to ensure that the correct people have access to the correct assets at the correct time.

- Data and Information

  This domain covers aspects about how to protect critical data in transit or at rest across the organization.

- Application and Process

  This domain covers aspects about how to ensure application and business services security.

- Network, Server and Endpoint (IT infrastructure)

  This domain covers aspects about how to stay ahead of emerging threats across IT system components.

- Physical Infrastructure

  This domain covers aspects about how to leverage the capability for digital controls to secure events—on people or things—in the physical space.

Let us now take a closer look at these domains.

1.4.2 People and Identity

Organizations need to protect the assets and services that serve the business and support the business operation. One aspect of protection is provided by *access control*. The ability to provide effective access control services is based on the ability to manage people and identity as defined by the enterprise's security governance, risk, and compliance model.

The Security Governance, Risk Management, and Compliance model provides guidance about how identities are managed and how access control is to be conducted. Organizations register people and map them to identities. The relationships between people and organization are expressed in terms of role, rights, business policies, and rules. The ability to register people and describe their relationship with the enterprise is a key security enabler for the remaining security domains:

- Data and Information
- Applications and Process
- Network, Server and Endpoint (IT infrastructure)
- Physical Infrastructure

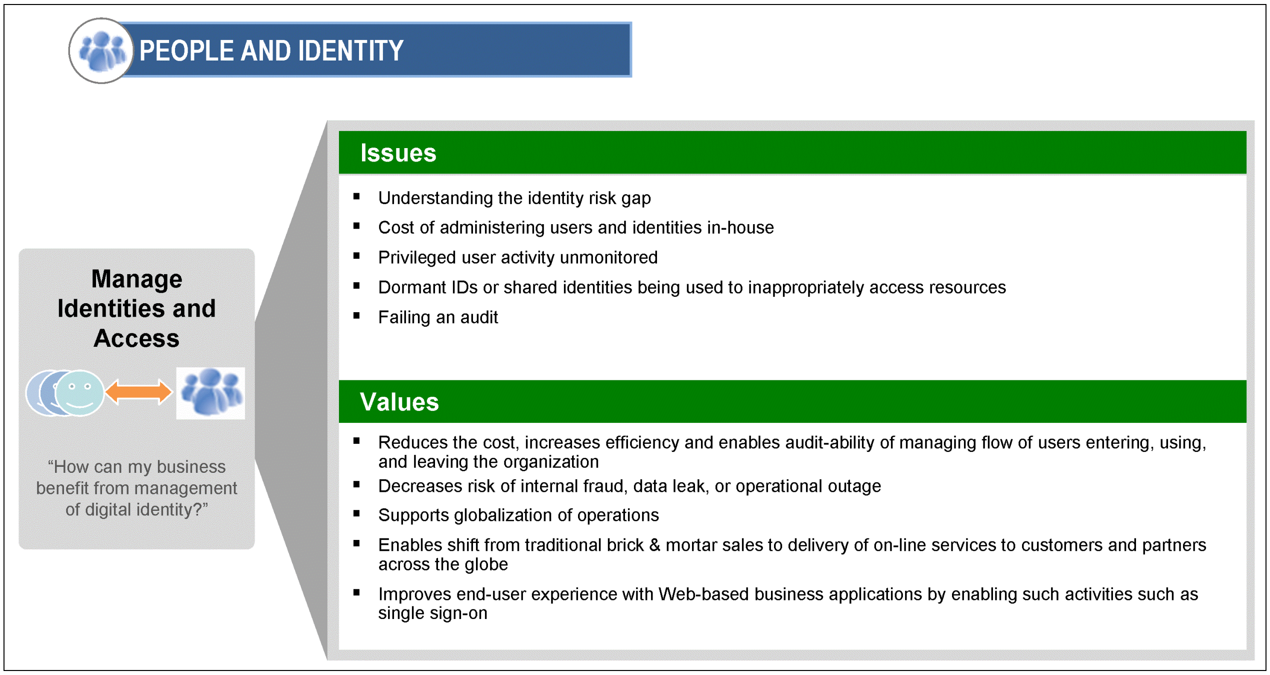
Operationally, people acting in authorized roles in an organization or as part of an extended relationship are granted access to infrastructure, data, information, and services. At the same time, people acting in unauthorized roles are denied access to infrastructure, data, information, and services if they are acting outside of the business policies and agreements.

Within an identity system, people can be issued a *credential*. A credential can take any of several forms, including a physical identity card or logical token or user identifier. The *trustworthiness* or *strength* of the credential is an important aspect of business policy and risk management. The ability to effectively manage the life cycle of identity, that is, the creation, removal, and role changes for dynamic populations of workforce, customer, or user communities, is extremely important. For example, the life cycle of identities and credentials can be influenced by business cycles, employment cycles, customer relationship, agreement, business, or calendar events, and so on.

Identity systems need to be integrated with appropriate sets of access controls. Identity systems need to manage user roles, rights, and privileges across the IT infrastructure that might contain multiple technology architectures, or multiple identity and access control systems will be required to ensure that users have access to the correct assets and services.

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

Figure 1-2 shows a summary and additional aspects to be addressed within the People and Identity domain.



PEOPLE AND IDENTITY

Manage Identities and Access

"How can my business benefit from management of digital identity?"

Issues

- Understanding the identity risk gap
- Cost of administering users and identities in-house
- Privileged user activity unmonitored
- Dormant IDs or shared identities being used to inappropriately access resources
- Failing an audit

Values

- Reduces the cost, increases efficiency and enables audit-ability of managing flow of users entering, using, and leaving the organization
- Decreases risk of internal fraud, data leak, or operational outage
- Supports globalization of operations
- Enables shift from traditional brick & mortar sales to delivery of on-line services to customers and partners across the globe
- Improves end-user experience with Web-based business applications by enabling such activities such as single sign-on

Figure 1-2 People and Identity domain

1.4.3 Data and Information

Organizations need to protect both the *raw data* and *contextualized information* that is within its span of control. The Security Governance, Risk Management, and Compliance model provides guidance about the value of data and information and how the risks to data and information must be managed.

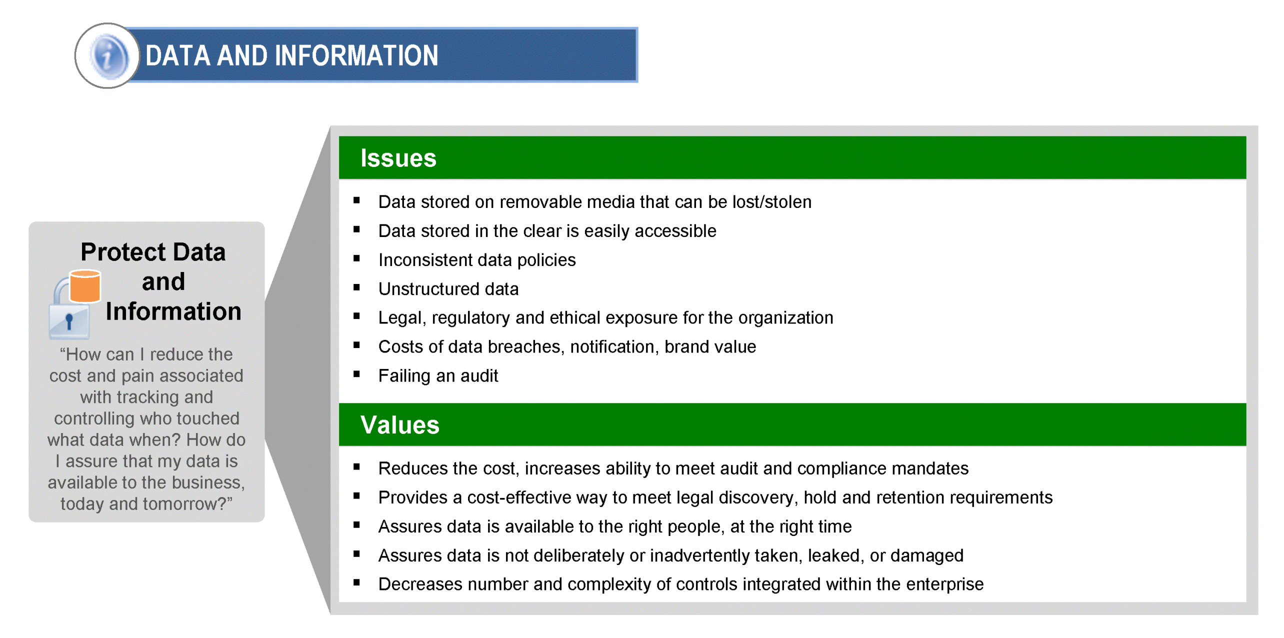
An effective plan for data and information protection includes maintaining a catalog or inventory of these assets, along with attributes, policies, and enforcement mechanisms and services that govern the access, transformation, movement, and disposition of data and information.

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 a full life cycle, from creation to destruction and across its various states, locations, and instantiations, and when it is stored or when it is being physically or electronically transported.

The term *data* can be applied to a wide range of electronically encoded assets. This includes software and firmware, which need to be protected against technical risks (to ensure that malicious code is not introduced) and business risks (to ensure that licensing terms have not been violated).

Protection of data and information is dependant on the definition and operation of all other operational security domains. Measuring and reporting on an organization's compliance with respect to 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 1-3 shows a summary and additional aspects to be addressed within the Data and Information domain.



DATA AND INFORMATION

Protect Data and Information

“How can I reduce the cost and pain associated with tracking and controlling who touched what data when? How do I assure that my data is available to the business, today and tomorrow?”

Issues

- Data stored on removable media that can be lost/stolen
- Data stored in the clear is easily accessible
- Inconsistent data policies
- Unstructured data
- Legal, regulatory and ethical exposure for the organization
- Costs of data breaches, notification, brand value
- Failing an audit

Values

- Reduces the cost, increases ability to meet audit and compliance mandates
- Provides a cost-effective way to meet legal discovery, hold and retention requirements
- Assures data is available to the right people, at the right time
- Assures data is not deliberately or inadvertently taken, leaked, or damaged
- Decreases number and complexity of controls integrated within the enterprise

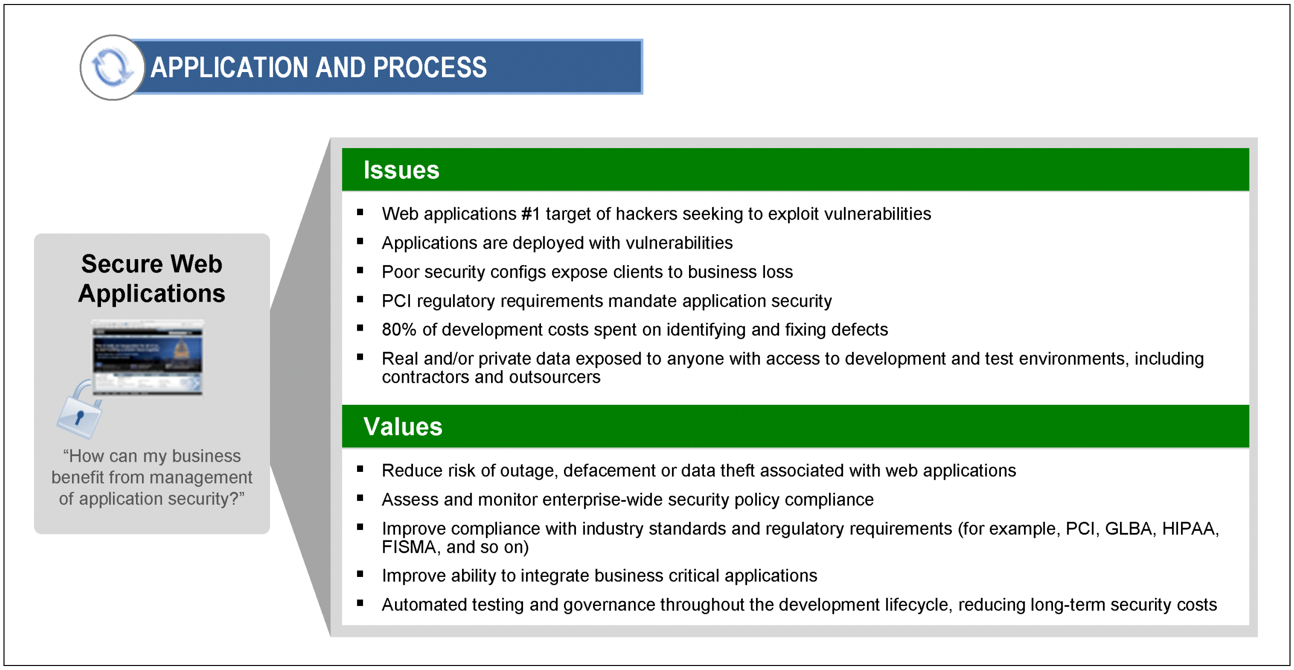
Figure 1-3 Data and Information domain

1.4.4 Application and Process

Organizations need to proactively protect their *business-critical applications* from external and internal threats throughout their entire life cycle, from design to implementation and production. Control throughout the application life cycle implies effective control and compliance in the remaining security domains. For example, whether an application is internally focused, such as a customer relationship management (CRM) system delivered through a service-oriented architecture (SOA), 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 is enabling the business rather than introducing additional risk.

Service management for all business and business support processes, including service management for processes within the security domain, is a critical part of ensuring that the business is operating within the appropriate risk management and compliance guidelines. Service management of security typically includes a combination of capabilities, such as centralized authentication, access and audit policy management, and web application vulnerability scanning and intrusion prevention.

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



APPLICATION AND PROCESS

Secure Web Applications

“How can my business benefit from management of application security?”

Issues

- Web applications #1 target of hackers seeking to exploit vulnerabilities
- Applications are deployed with vulnerabilities
- Poor security configs expose clients to business loss
- PCI regulatory requirements mandate application security
- 80% of development costs spent on identifying and fixing defects
- Real and/or private data exposed to anyone with access to development and test environments, including contractors and outsourcers

Values

- Reduce risk of outage, defacement or data theft associated with web applications
- Assess and monitor enterprise-wide security policy compliance
- Improve compliance with industry standards and regulatory requirements (for example, PCI, GLBA, HIPAA, FISMA, and so on)
- Improve ability to integrate business critical applications
- Automated testing and governance throughout the development lifecycle, reducing long-term security costs

Figure 1-4 Application and Process domain

1.4.5 Network, Server and Endpoint

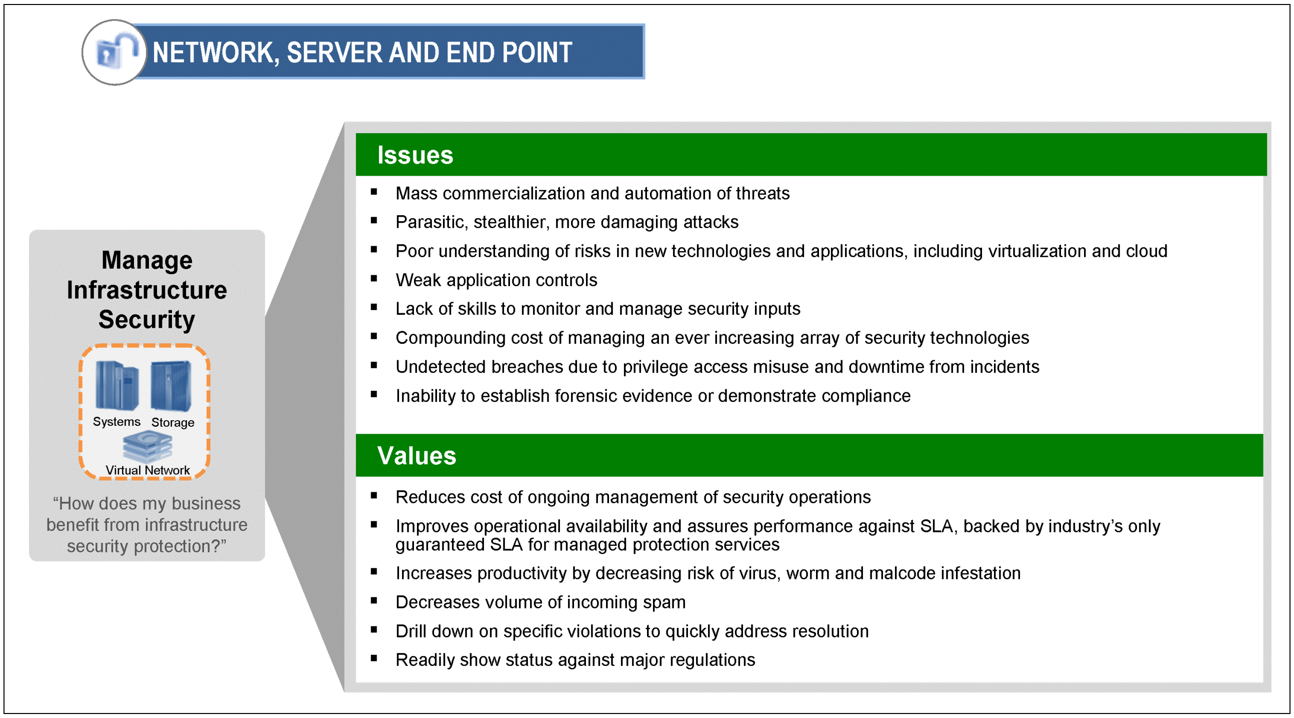
Organizations need to *preemptively* and *proactively monitor* the operation of the business and the IT infrastructure for *threats* and *vulnerabilities* to avoid or reduce breaches.

The Security Governance, Risk Management, and Compliance model can provide guidance on the business implications of technology-based risks. In practice, the definition, deployment, and management of technology-based threats, as well as the technical aspects of incident response, can be delegated to operational management and staff, or outsourced to a service provider.

Security monitoring and management of an organization's network, server, 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 network infiltrations. While no technology is perfect, the focus and intensity of security, monitoring, and management can be affected by the type of network, server, and endpoints deployed in the IT infrastructure and how those components are built, integrated, tested, and maintained.

Organizations leverage *virtualization technology* to support their goals of delivering services in less time and with greater agility. 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 gaining peace of mind that the virtual systems are secured with the same rigor as the physical systems.

Figure 1-5 shows a summary and additional aspects to be addressed within the Network, Server and Endpoint domain.


NETWORK, SERVER AND END POINT

Manage Infrastructure Security

"How does my business benefit from infrastructure security protection?"

Issues

- Mass commercialization and automation of threats
- Parasitic, stealthier, more damaging attacks
- Poor understanding of risks in new technologies and applications, including virtualization and cloud
- Weak application controls
- Lack of skills to monitor and manage security inputs
- Compounding cost of managing an ever increasing array of security technologies
- Undetected breaches due to privilege access misuse and downtime from incidents
- Inability to establish forensic evidence or demonstrate compliance

Values

- Reduces cost of ongoing management of security operations
- Improves operational availability and assures performance against SLA, backed by industry's only guaranteed SLA for managed protection services
- Increases productivity by decreasing risk of virus, worm and malcode infestation
- Decreases volume of incoming spam
- Drill down on specific violations to quickly address resolution
- Readily show status against major regulations

Figure 1-5 Network, Server and Endpoint domain

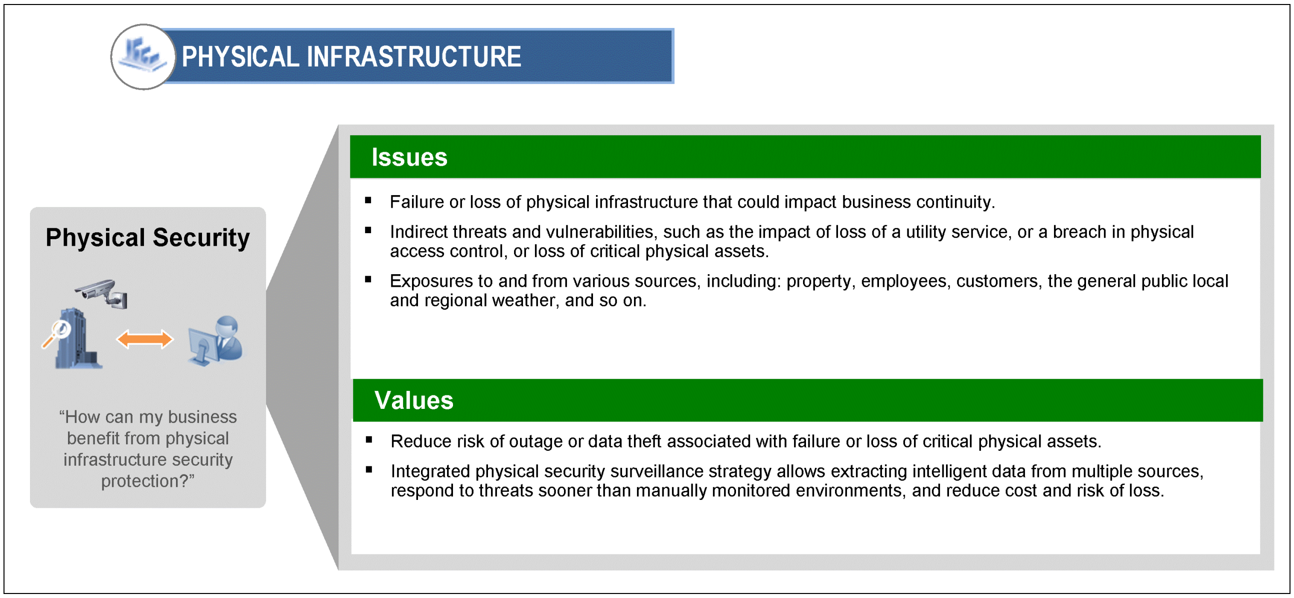
1.4.6 Physical Infrastructure

For an organization to effectively implement an enterprise security plan, the business and technical risks that are associated with the physical infrastructure must be understood and addressed. Security Governance, Risk Management, and Compliance provides guidance on the types of risks and the types of plans and responses for physical security.

Protecting an organization's infrastructure can mean taking precautions against a failure or loss of physical infrastructure that might impact business continuity. Protecting an organization's infrastructure can involve protection from indirect threats and vulnerabilities, such as the impact of loss of a utility service, a breach in physical access control, or 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 weather.

For example, securing the perimeter of the data center with cameras and centralized monitoring devices is critical to ensure managed access to an organization's IT assets. Therefore, organizations concerned about theft and fraud, such as banks, retail stores, or public agencies, should define and implement an integrated physical security surveillance strategy that includes monitoring, analytics, and centralized control. This approach enables organizations to extract intelligent data from multiple sources and respond to threats sooner than manually monitored environments, resulting in reduced cost and risk of loss.

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



PHYSICAL INFRASTRUCTURE

Physical Security

“How can my business benefit from physical infrastructure security protection?”

Issues

- Failure or loss of physical infrastructure that could impact business continuity.
- Indirect threats and vulnerabilities, such as the impact of loss of a utility service, or a breach in physical access control, or loss of critical physical assets.
- Exposures to and from various sources, including: property, employees, customers, the general public local and regional weather, and so on.

Values

- Reduce risk of outage or data theft associated with failure or loss of critical physical assets.
- Integrated physical security surveillance strategy allows extracting intelligent data from multiple sources, respond to threats sooner than manually monitored environments, and reduce cost and risk of loss.

Figure 1-6 Physical Infrastructure domain

After having addressed and mapped the IT security domains into your business solutions, it is time to look at the component-oriented view of IT security in the IT Security Blueprint.

1.5 IBM Security Blueprint

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

The IBM Security Blueprint uses a product-agnostic and solution-agnostic 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 researching many customer-related scenarios, focusing on how to build IT solutions. The intention of the blueprint is to support and assist in designing and deploying 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, 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 has chosen to use a high-level service-oriented perspective for the blueprint, 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 1-7.

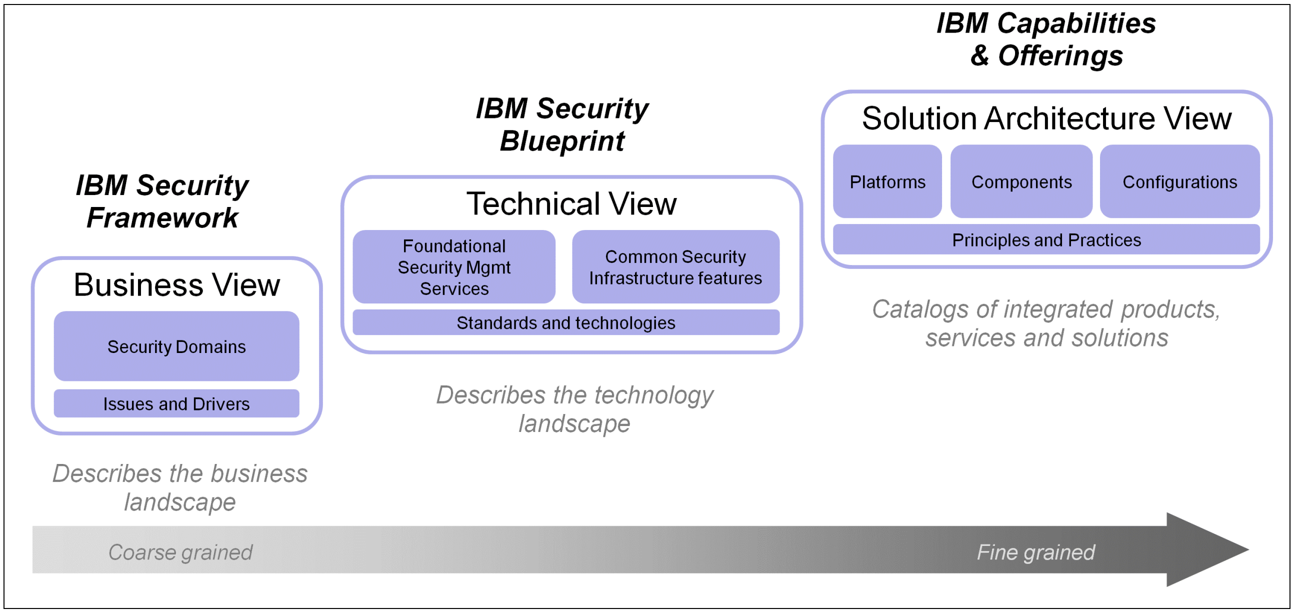

IBM Capabilities & Offerings
Solution Architecture View
Platforms
Components
Configurations
Principles and Practices
Catalogs of integrated products, services and solutions
IBM Security Blueprint
Technical View
Foundational Security Mgmt Services
Common Security Infrastructure features
Standards and technologies
Describes the technology landscape
IBM Security Framework
Business View
Security Domains
Issues and Drivers
Describes the business landscape
Coarse grained
Fine grained

Figure 1-7 IBM Security Blueprint positioning

The left portion of Figure 1-7 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 1-7 represents the IBM Security Blueprint, which describes the IT security management and IT security infrastructure capabilities needed in an organization. As discussed earlier, the IBM Security Blueprint describes these capabilities in product and vendor-neutral terms.

The right portion of Figure 1-7 represents the solution architecture views, which describe specific deployment guidance particular to a given IT environment. Solution architecture views provide details about specific products, solutions, and their interactions.

Figure 1-8[5] shows the complete IBM Security Blueprint, and each layer and component are described in the following sections.

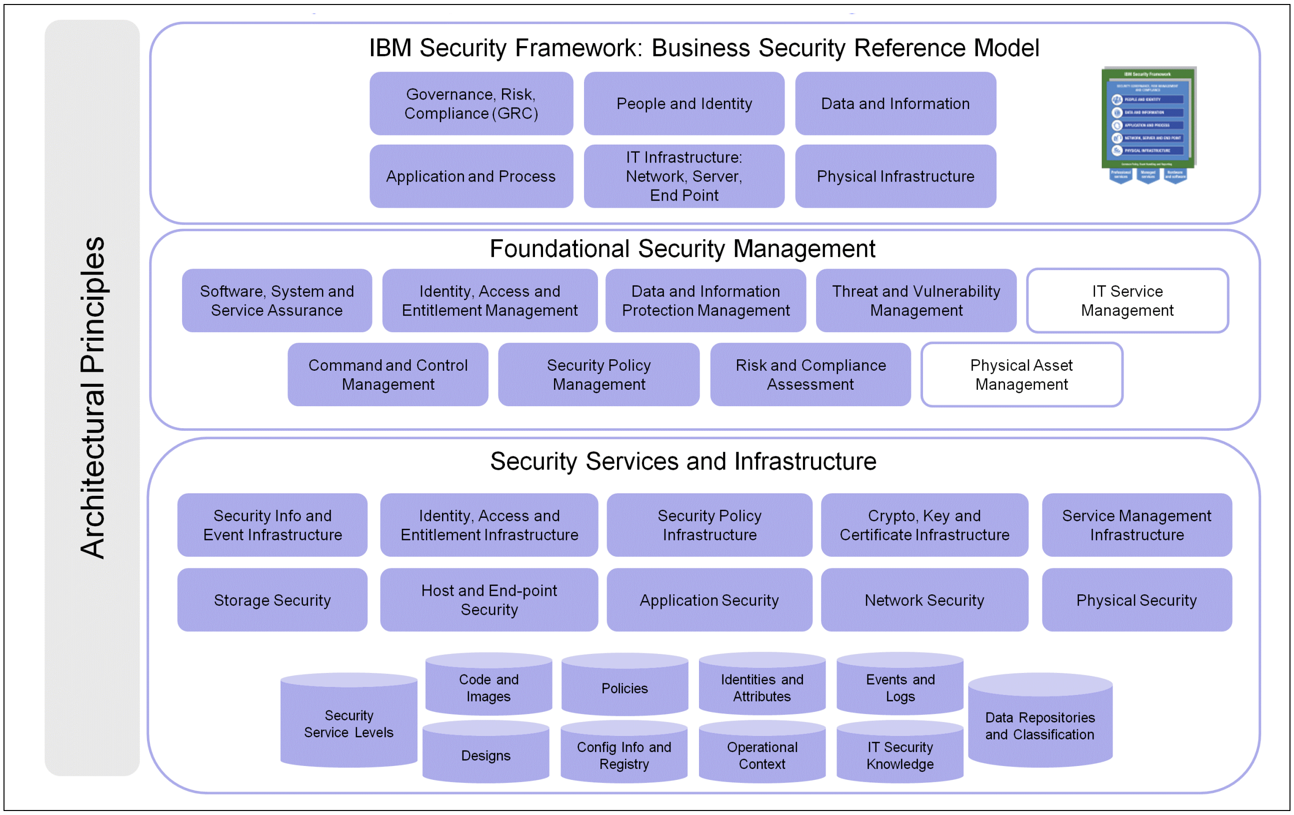

Architectural Principles
IBM Security Framework: Business Security Reference Model
Governance, Risk, Compliance (GRC)
People and Identity
Data and Information
Application and Process
IT Infrastructure: Network, Server, End Point
Physical Infrastructure
Foundational Security Management
Software, System and Service Assurance
Identity, Access and Entitlement Management
Data and Information Protection Management
Threat and Vulnerability Management
IT Service Management
Command and Control Management
Security Policy Management
Risk and Compliance Assessment
Physical Asset Management
Security Services and Infrastructure
Security Info and Event Infrastructure
Identity, Access and Entitlement Infrastructure
Security Policy Infrastructure
Crypto, Key and Certificate Infrastructure
Service Management Infrastructure
Storage Security
Host and End-point Security
Application Security
Network Security
Physical Security
Security Service Levels
Code and Images
Designs
Policies
Config Info and Registry
Identities and Attributes
Operational Context
Events and Logs
IT Security Knowledge
Data Repositories and Classification

Figure 1-8 The IBM Security Blueprint

1.5.1 Foundational Security Management

The Foundational Security Management layer contains the top-level components 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 23.

Let us take 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. 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 non-IT assets and services to ensure protection, response, continuity, and recovery. 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

[5] White boxes in Figure 1-8 on page 17 and other diagrams represent services or components that are not solely security related but might be connected with other IT service areas as well.

  - 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 services and repositories to author, discover, analyze, transform, distribute, evaluate, and enforce security policies.
- *Identity, Access, and Entitlement Management* provides services related to roles and identities, access rights, and entitlements. The proper use of these services can ensure that access to resources has been 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 use.
- *Data and Information Protection Management* provides services 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 life cycle 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
  - 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 services 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.
- *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 sub-components that are being utilized 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, 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 (OSs) 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 can include employee badges, RFID readers, surveillance systems, and associated technology or assets. Physical Security can include automation 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 have defined the following *Architectural Principles* that accompany the service decomposition. These 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. This includes support for all major platforms, run times, and languages, support for major industry standards, published interfaces and algorithms, no 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, but security policies must be secure out-of-the box. This 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.

  In today's environments, 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 requires flexible support for the constraints set by government regulations and industry standards and traceability between regulations, standards, and business policies and the security policies used to implement them.

- Design for privacy.

  In the current age of data sharing, privacy becomes increasingly important. Solutions must highlight the use 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 a variety of mechanisms under the same framework. Already 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 made in terms of span of control.

- Design for consumability.

  All security services must be easily used by a variety of audiences. This includes 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 must be aware of their security context.

  Resources and actors are kept aware of their environment (including physical location and logical co-location) and their security status and context.

- Security is model-driven.

  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 gets broken (plus, they increase management impact).

  The IBM Security Blueprint lists the preferred standards and mechanisms.

This concludes the overview of the IBM Security Blueprint. In the next section, we discuss the components of the IBM Security Blueprint in more detail.

2

The components of the IBM Security Blueprint

In this section we explain the IBM Security Blueprint in more detail by discussing the *components* and *subcomponents* of the IBM Security Blueprint.

The components in the IBM Security Blueprint describe the common security capabilities 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 agnostic 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 agnostic 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. While this section provides many details about the first layer, the second, more supportive layer is discussed more briefly because many terms should be familiar to the information technology (IT) security professional.

2.1 Foundational Security Management

In this section we explain 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 form a closed loop management system. Figure 2-1 depicts the continues risk management cycle as it has to be practiced for comprehensive security management. *Command and Control Management* sets security directives and objectives, which are used by *Security Policy Management* to produce and set the policies and standards that have to be adhered to in the other functional areas of security, as they are represented on the right side of Figure 2-1.

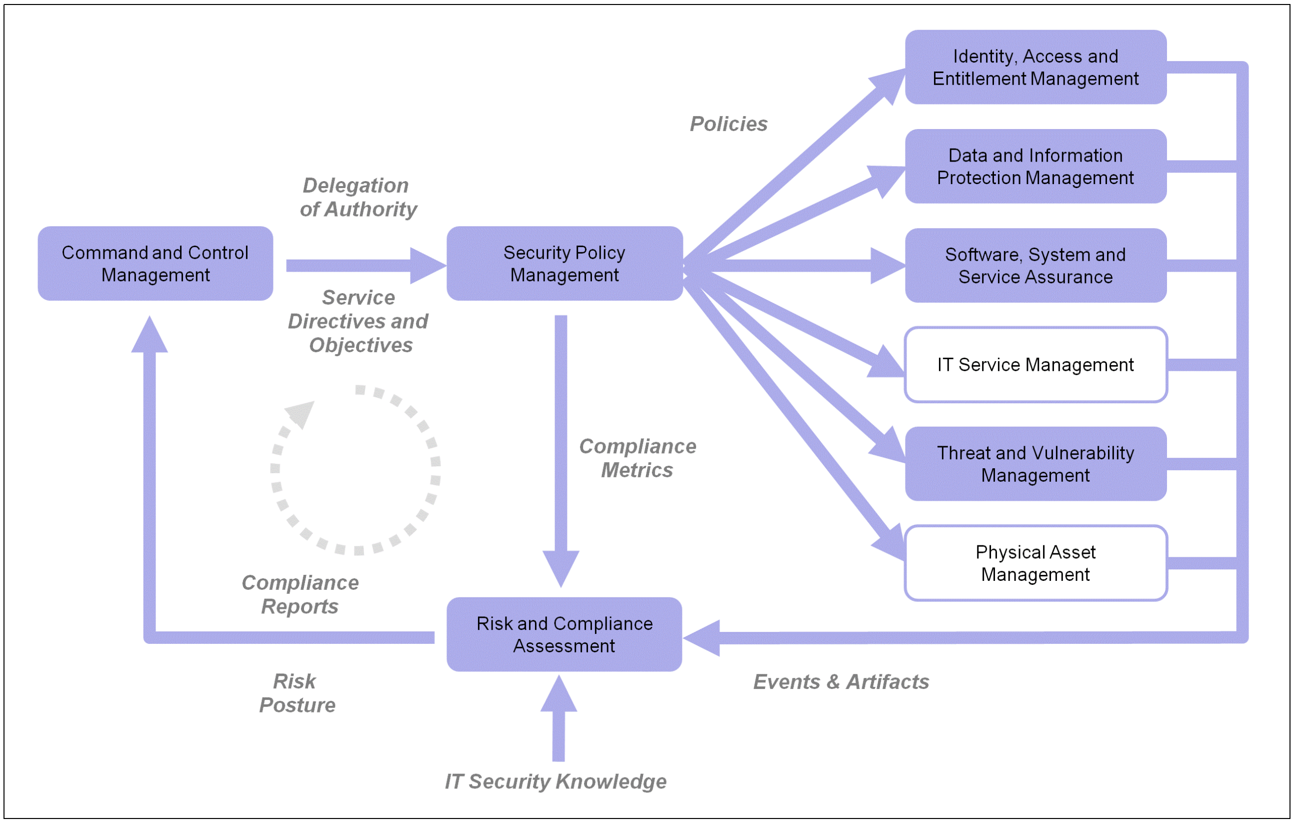

Policies
Delegation of Authority
Command and Control Management
Security Policy Management
Service Directives and Objectives
Identity, Access and Entitlement Management
Data and Information Protection Management
Software, System and Service Assurance
IT Service Management
Threat and Vulnerability Management
Physical Asset Management
Compliance Metrics
Compliance Reports
Risk and Compliance Assessment
Risk Posture
Events & Artifacts
IT Security Knowledge

Figure 2-1 Foundational security 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 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, with the exception of the

Application and Process domain, which is matched by the Software, Systems, and Service Assurance component and the IT Service Management component.

In the next section we provide 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*, as well as an alignment of key Security Services and Infrastructure components, which are essential to a given component 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, such as:

- 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 utilize 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[1] shows an overview of Command and Control Management components and the related components from the Security Services and Infrastructure layer.

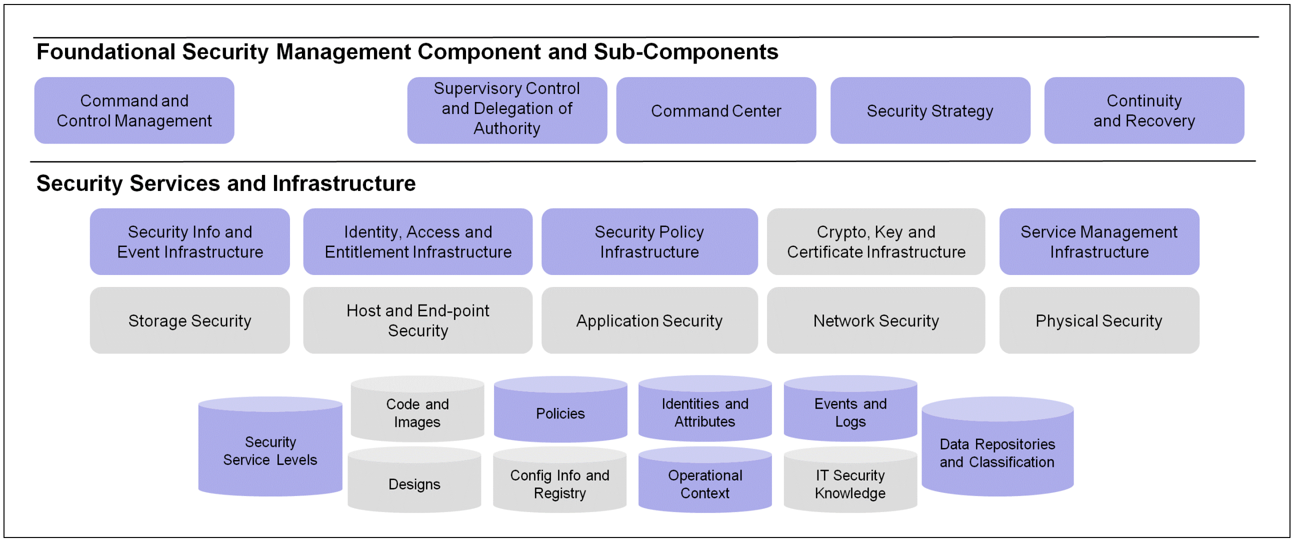

Foundational Security Management Component and Sub-Components
Command and Control Management
Supervisory Control and Delegation of Authority
Command Center
Security Strategy
Continuity and Recovery
Security Services and Infrastructure
Security Info and Event Infrastructure
Identity, Access and Entitlement Infrastructure
Security Policy Infrastructure
Crypto, Key and Certificate Infrastructure
Service Management Infrastructure
Storage Security
Host and End-point Security
Application Security
Network Security
Physical Security
Security Service Levels
Code and Images
Designs
Policies
Config Info and Registry
Identities and Attributes
Operational Context
Events and Logs
IT Security Knowledge
Data Repositories and Classification

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

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[2] (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 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 travelling for the company and knowing to whom authority should be delegated if a person becomes incapacitated or otherwise unavailable.

[1] Gray boxes in Figure 2-2 and other diagrams represent services or components that are not required for a respective tasks.

[2] To learn more about SCADA see http://www.cpni.gov.uk/ProtectingYourAssets/scada.aspx.

Command Center

The Command Center represents the service organization unit 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 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.

Continuity and Recovery

Continuity and Recovery represents a service applying 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, as well as 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 2.2.1, “Command and Control Management” on page 25 (depicted as blue-shaded objects in Figure 2-2 on page 26):

- Identity, Access, and Entitlement Infrastructure

  The Identity, Access, and Entitlement Infrastructure is used by all services in 2.2.1, “Command and Control Management” on page 25, to delegate authority by authorizing appointed personnel to receive respective access rights.

- Security Policy Infrastructure

  Security Policy Infrastructure is a key component for 2.2.1, “Command and Control Management” on page 25, 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 confirming 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 can be valuable when the command center needs to confirm ad hoc occurrences of specific events during crisis management or in discussions with authorities.

- 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 associated with the Command and Control Management services are also actors in the Service Management Infrastructure processes. For instance, a change with an impact on security might have to 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) has not been properly 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 define the roles within the organization used in describing policies developed in Command and Control Management.

- Operational Context

  Operational Context refers to the existing procedures and policies 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 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 security requirements needed to mitigate business risks into an IT perspective, which can then be consumed and enforced by the IT infrastructure.

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

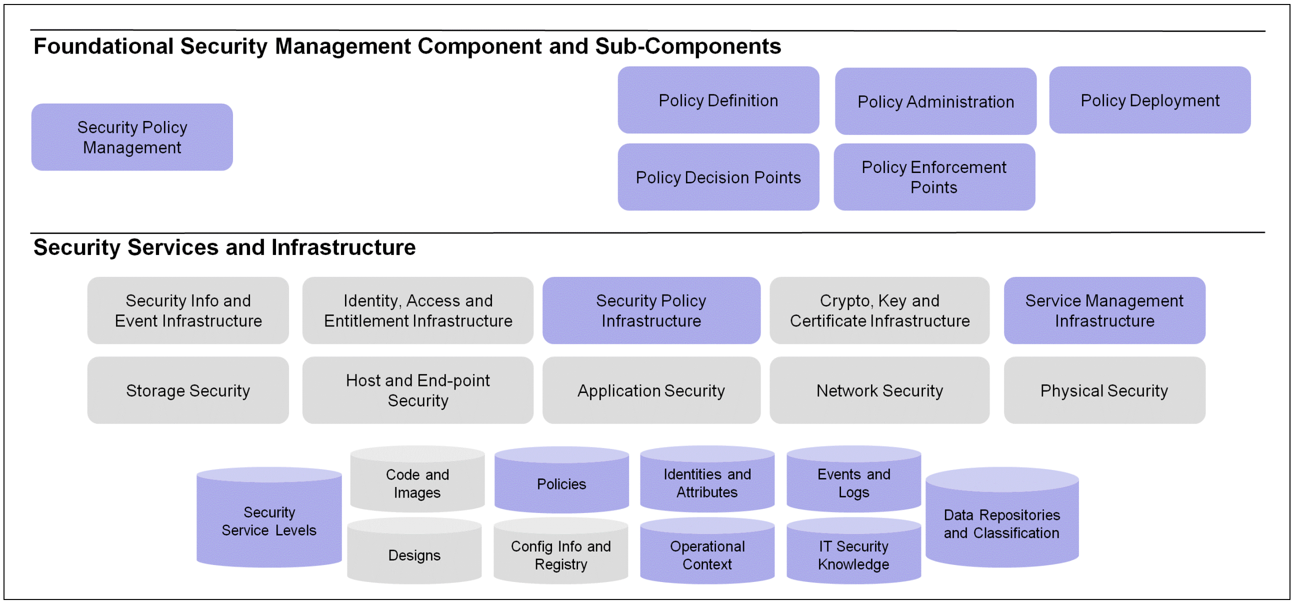

Foundational Security Management Component and Sub-Components
Security Policy Management
Policy Definition
Policy Administration
Policy Deployment
Policy Decision Points
Policy Enforcement Points
Security Services and Infrastructure
Security Info and Event Infrastructure
Identity, Access and Entitlement Infrastructure
Security Policy Infrastructure
Crypto, Key and Certificate Infrastructure
Service Management Infrastructure
Storage Security
Host and End-point Security
Application Security
Network Security
Physical Security
Security Service Levels
Code and Images
Designs
Policies
Config Info and Registry
Identities and Attributes
Operational Context
Events and Logs
IT Security Knowledge
Data Repositories and Classification

Figure 2-3 Security Policy Management subcomponents

Security Policy Management consists of the following subcomponents:

- Policy Definition
- Policy Administration
- Policy Deployment
- Policy Decision Points
- Policy Enforcement Points

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

Policy Definition

The Policy Definition subcomponent represents the ability to represent an IT security policy in human-readable terms, a machine-readable format, or both. It represents the translation of security directives and objectives—as derived by the Command and Control Management from the business security requirements—into actions that can be taken and enforced in the IT landscape. The policies are in scope on all levels and include the top-level security directive, underlying general security policies, deriving more technical policies and platform-specific security standards, in addition to related guidelines and procedures.

The Policy Definition is responsible for capturing the context and background of the IT security policy by tracking the *upstream* policy documents that influence it or rationalize and justify it.

Policy Administration

Policy Administration addresses the human-oriented workflow processes within the policy life cycle management, which includes the 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 Deployment. Also, related activities for this subcomponent include policy education and security awareness.

Policy Deployment

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

For machine-readable policies, the policies are defined centrally and are 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 then transformed at the enforcement point to a local representation so that they can be enforced.

Policy Decision Points

Policy Decision Points (PDPs) represent the capability to evaluate a request and make a decision about whether the request is conformant to a policy. In certain cases, all the information 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 affecting the placement of PDPs in an IT environment. Centralization of the PDPs reduces administrative burdens and potential errors during deployment. Centralization of the PDPs also enables 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) take action based on whether the request conforms to policy. The action might be an enforcement action, permitting or denying the request. The PEP might also monitor, log, and raise alerts without affecting the request.

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 29):

- Security Policy Infrastructure

  The Security Policy Infrastructure is the key component 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, have to 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 set for an environment should be achievable to a large extent, so it is important to establish the targeted controls documented in the policies with consideration of their achievability and their appropriateness. The Operational Context provides essential input for related evaluations of controls. This also helps to avoid the situation in which a policy would have to 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 set out in the policies. An unnecessary number of exceptions also requires a lot of 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 given to establish appropriate, practical, achievable control requirements in the policies, exceptions in an operational environment are unavoidable. Such exceptions can derive, for instance, from the lack of support of a given control by a particular system. While 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 as 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, a sufficient yet manageable set of classifications of information assets has to 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 above, the Data Repositories and Classifications are also examined as part of Policy Administration for the evaluation of exceptions from policy-mandated controls usually required for a given data repository in cases in which such controls cannot be maintained for technical or business reasons.

- Identities and Attributes

  Besides the Operational Context, Data Repositories and Classifications, Identities and Attributes represent another data item that has to be fully understood to define appropriate policies for a given environment. While the Operational Context helps to evaluate the environment from a business and technical infrastructure perspective, and Data Repositories and Classifications help 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 actioners in the environment.

  Like 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 will use Identities and Attributes and its evolvement 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 completion of Security Policy Management activities, which have been performed with the help of the Security Policy Infrastructure. From this perspective, the Events and Logs serve as evidential records about activities (for instance, whether a specific control has received review and approval from stakeholders as part of Policy Administration activities before it is published in an updated security policy). But also from a perspective of Policy Definition, Events and Logs can be a helpful source of information. Alongside the traditional qualitative analysis of Operational Context, Data Repositories and Classifications, and Identities and Attributes when defining 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 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 following 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 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 have to be established to provide clearer direction towards the implementation of respective policies. Also, general knowledge about well-established industry regulations and standards as well as about data privacy regulations in the various legal contexts in which a organization operates is required to better translate related directives and objectives coming from the business via Command and Control Management into the respective policies.

2.2.3 Risk and Compliance Assessment

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 might contribute to an organization’s operational risk. This component covers risk aggregation and reporting, IT security risk processes, business controls management, resiliency and continuity management, compliance reporting, and legal discovery 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.

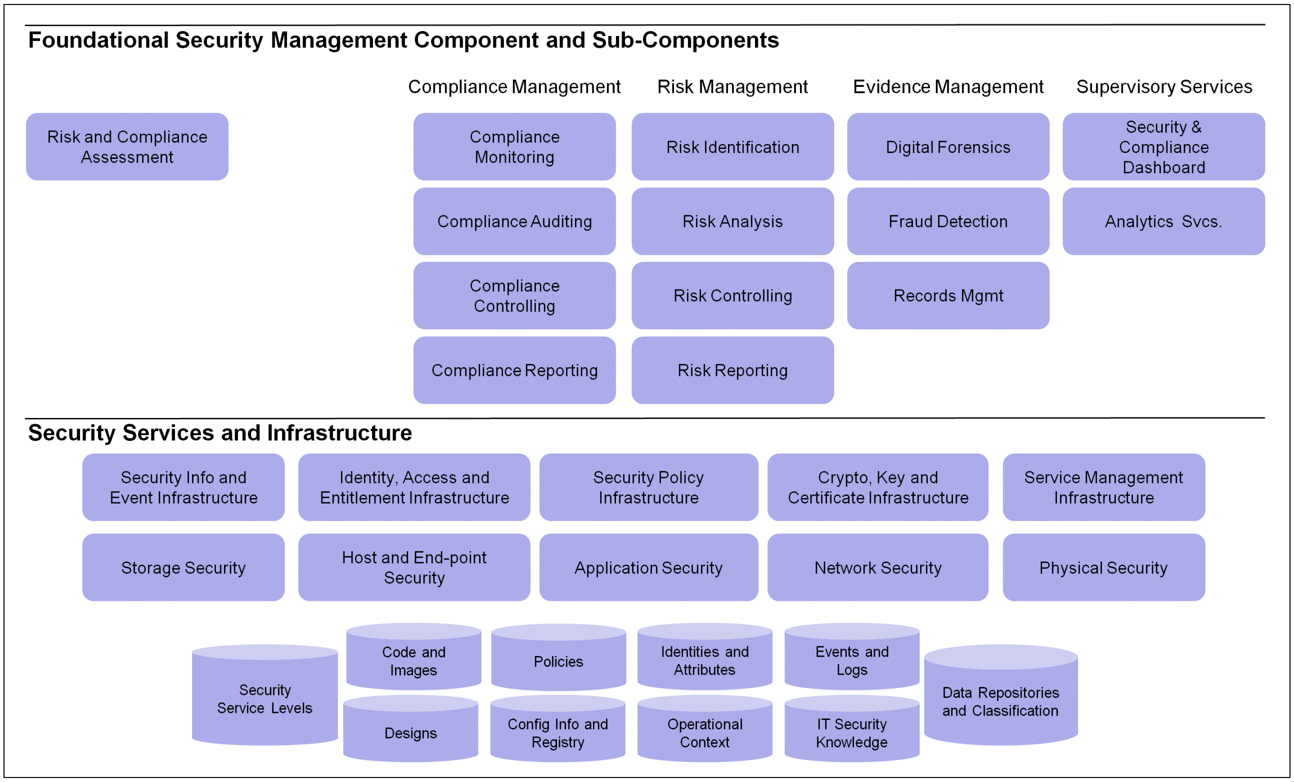


Figure 2-4 Risk and Compliance Assessment subcomponents

Risk and Compliance Assessment consists of the following subcomponents:

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

These four services are discussed in more detail in the following sections.

Compliance Management

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

Compliance Monitoring

Compliance Monitoring refers to 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 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 than 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 those 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 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 have to 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 activities 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 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 given 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 have to 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 has to 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 involves preserving the state of a system for future reference. In other cases, forensics requires 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 time line of configuration changes for a database might need to be recreated 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, additional 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 relating 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 have been collected over a period of time.

Analytics Services

Analytics Services help to find trends in correlated events and to make decisions based on the trends found. For example, an event analytics engine might match authorization events against human resources employee records to detect the use of orphaned accounts for people who have 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 events 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 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 33):

- Security Information and Event Infrastructure

  The Security Information and Event Infrastructure is an important element for the 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 specifically designed for compliance to particular regulation and legal requirements. This infrastructure component also provides a substantial part of the evidence that has to be gathered and analyzed by the Evidence Management services.

  Besides providing services *for* the 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 pertaining 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 resulting from malicious user behavior.

Besides providing services *for* the 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 proper 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 given point in time, but it supports the evolution of policies and standards. It allows the recording of the state of approval for a given policy at a given point in time and provides convenient ways to examine differences between various compliance requirements. This 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 has been properly 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 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 utilize the Cryptography, Key, and Certificate Infrastructure have to 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 needs to be thoroughly assessed by the Compliance Management pillar.

- Service Management Infrastructure

  Risk and Compliance Assessment services operate under an agreed-upon Service Management Infrastructure and must utilize the services provided by that infrastructure. For example, accessing and transferring evidence from audited machines must be performed in line with the change management process (for instance, they must utilize proper change management ticketing and approval, and thus use the Service Management Infrastructure). Equally important, Evidence Management activities have to be performed in line with incident and problem management processes and utilize the related parts of the Service Management Infrastructure (for instance, mechanisms 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. This means that Storage Security is assessed and examined by these services.

From an indirect perspective, Storage Security is heavily utilized by all five aforementioned 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 via 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 have to 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, Eost 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 have to be analyzed for risk and compliance. Because it is the closest, most used interface to the business user, it is important that it be examined for Compliance Management and Evidence Management, especially for fraudulent activities.

- Network Security

  Like many of the other technical platforms, network components and traffic provides 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 have to be functional to fulfill compliance requirements in mitigate risks and retain evidence.

  Physical Security is essential because information that must be protected does not only exist 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 as well as the security control objectives 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 need to 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 only surface 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 have to 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 has been 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 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 have to be implemented to meet security controls defined in the policies. Compliance Management uses this information to verify that the security controls are properly 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 to the extent as this 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 deriving from errors in Identities and Attributes. While 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 have been bypassed to make changes on Identities and Attributes. The Evidence Management services require access to Identities and Attributes to gather evidence about identities that have been 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. In other words, 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 given user for a given resource are appropriate from a compliance and risk perspective. For instance, information access should not be granted to a user with specific *identity features* like 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 (four-eye-principle).

- Operational Context

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

  An example for such influence can be the execution of privileged activities with an unrestricted account. While an administrator might be granted—from a technical perspective—unrestricted access to a system, this administrator should only use a limited subset of commands to perform a given change. Hence, the execution of other privileged commands 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 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 has to 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 related to roles and identities, access rights, and entitlements. The proper use of these services can ensure that access to resources has been 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 use.

Figure 2-5 shows an overview of Risk and Compliance Assessment subcomponents and the related components from the Security Services and Infrastructure layer.

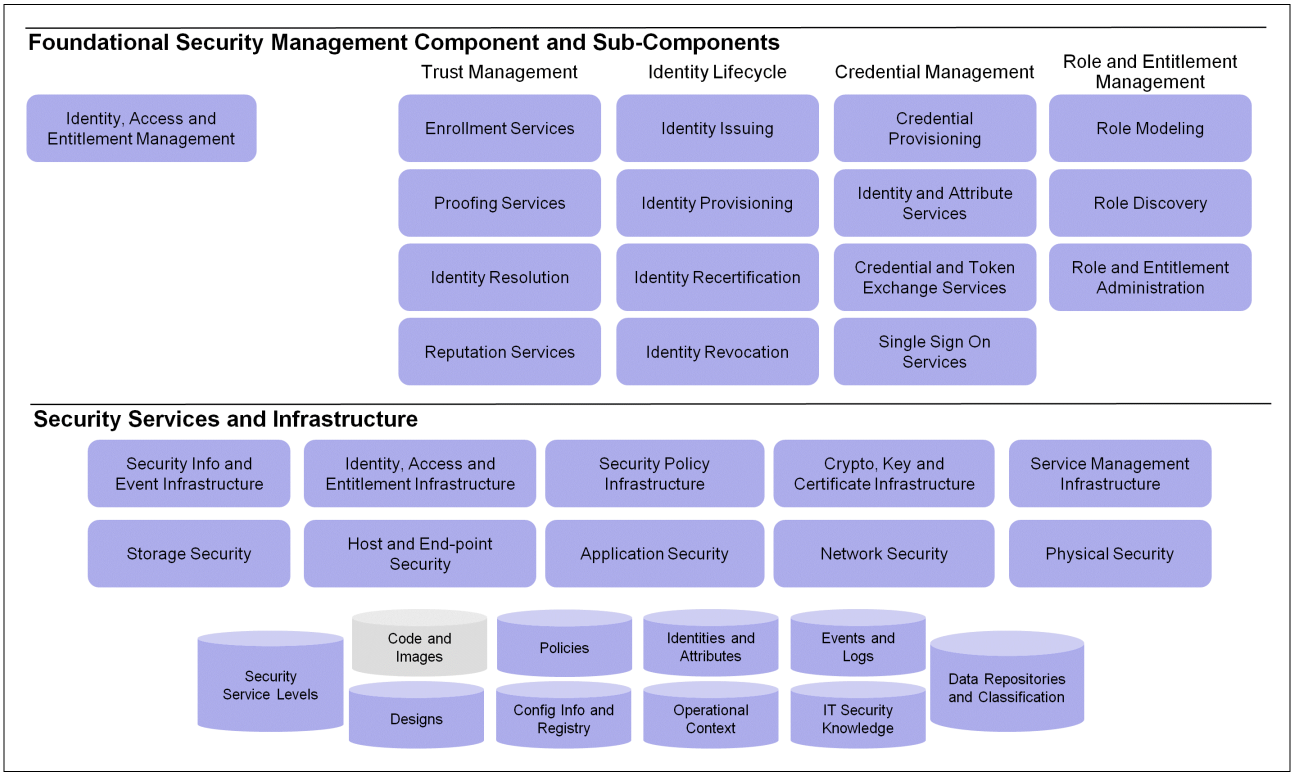

Foundational Security Management Component and Sub-Components
Trust Management
Identity Lifecycle
Credential Management
Role and Entitlement Management
Identity, Access and Entitlement Management
Enrollment Services
Identity Issuing
Credential Provisioning
Role Modeling
Proofing Services
Identity Provisioning
Identity and Attribute Services
Role Discovery
Identity Resolution
Identity Recertification
Credential and Token Exchange Services
Role and Entitlement Administration
Reputation Services
Identity Revocation
Single Sign On Services
Security Services and Infrastructure
Security Info and Event Infrastructure
Identity, Access and Entitlement Infrastructure
Security Policy Infrastructure
Crypto, Key and Certificate Infrastructure
Service Management Infrastructure
Storage Security
Host and End-point Security
Application Security
Network Security
Physical Security
Security Service Levels
Code and Images
Designs
Policies
Config Info and Registry
Identities and Attributes
Operational Context
Events and Logs
IT Security Knowledge
Data Repositories and Classification

Figure 2-5 Identity, Access and Entitlement Management subcomponents

Identity, Access and Entitlement Management consists of the following subcomponents:

- Trust Management
- Identity Life cycle
- Credential Management
- Role and Entitlement Management

These services are explained in the next sections.

Trust Management

Trust Management refers to the activities 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 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 of 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 Life cycle

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

Identity Provisioning

Identity Provisioning covers the processes and technology used to create the credential that will be used when issuing an identity token (for example, national ID card) and registering the credential to systems that need to authenticate the credential.

Identity Issuing

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

Identity Recertification

Identity Recertification refers to the processes and technology used to re-validate a credential that has already been issued. In certain cases, this means updating the credential itself. For example, a digital certificate has expired and another one has to be issued. In other cases, the recertification involves re-authorization and presenting proofing materials again.

Identity Revocation

Identity Revocation covers the processes and technologies used to de-certify a credential so that it can no longer be used as an identity token. This 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, like 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 life cycle.

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 evaluating user-presented authentication credentials and to build privilege credentials used by session management services. The privileges are typically based on attributes of a user stored in the Identities and Attributes security service, such as group membership, roles, personal attributes, and so on.

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 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 designed to remove the burden of repeating actions 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 requesting information about the requestor.

These identity providers (IPs) are trusted third parties and need to 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 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 and is less error prone when enforcing 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 either manually by observation and analysis of processes and interviews of the process actioner or process owners. Information can also be captured from systems supporting 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 identifies.

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 41):

- Security Info 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 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 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 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 used in an authentication request have been signed or encrypted so that a Policy Decision Point can properly validate the credentials. The Cryptography, Key and Certificate Infrastructure provides the ability to 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. End-point 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 established by the end-point often need to be propagated to back-end systems or translated into equivalent credentials used in back-end systems. Likewise, the end-points 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 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 be 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 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 Info 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 contains information about people 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 current organizational structure for the enterprise. The Identity, Access and Entitlement Management system relies on the directories when mapping organizational roles to application roles and other sorts of entitlements.

- 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 has been 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 access and data loss, according to the nature and business value of information. It also provides usage and access monitoring and audit services.

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

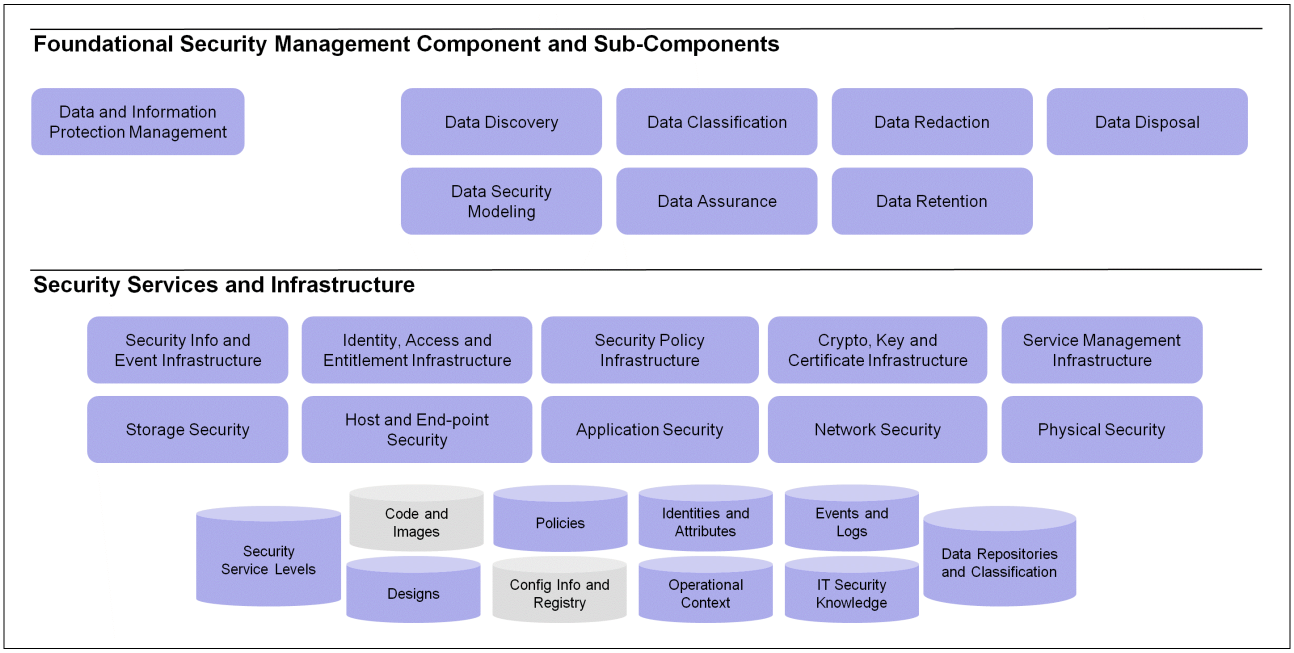

Foundational Security Management Component and Sub-Components
Data and Information Protection Management
Data Discovery
Data Classification
Data Redaction
Data Disposal
Data Security Modeling
Data Assurance
Data Retention
Security Services and Infrastructure
Security Info and Event Infrastructure
Identity, Access and Entitlement Infrastructure
Security Policy Infrastructure
Crypto, Key and Certificate Infrastructure
Service Management Infrastructure
Storage Security
Host and End-point Security
Application Security
Network Security
Physical Security
Security Service Levels
Code and Images
Designs
Policies
Config Info and Registry
Identities and Attributes
Operational Context
Events and Logs
IT Security Knowledge
Data Repositories and Classification

Figure 2-6 Data and Information Protection Management subcomponents

Data and Information Protection Management consists of the following subcomponents:

- Data Discovery
- Data Security Modeling
- Data Classification
- Data Assurance
- Data Redaction
- Data Retention
- Data Disposal

These services are explained in the following sections.

Data Discovery

The first step in securing data is having an accurate inventory of the organization's data repositories and understanding the security risks 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.

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 has been applied to data as it has been moved among repositories.

Building the business object view and understanding the transforms that the data has been subject to are key to planning master data management processes and business object archiving.

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 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.

Logical data models are the semantic hub of an enterprise architecture. Logical data models are sometimes overlooked in the software development life cycle, but they have become 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 attached to them that define requirements for confidentiality and encryption, access control, obfuscation, and redaction.

Data Classification

Data Classification refers to the tools and processes used to create a common set of semantic tags used by data modelers, data analysts, business analysts, governance stewards, and data architects.

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 expressed in terms of the logical data model. For example, a *high value customer* might be defined as a customer who has 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 helps 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 Assurance

Data Assurance refers to tools and activities to make sure 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 Redaction

Data Redaction refers to a set of tools and methods for eliminating sensitive or confidential data from a data set 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.

A variety of 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 enabling the release of related and relevant data.

Data Retention

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

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

After archived, the snapshot files can remain on the local storage media or can be deleted. The organization controls how long an archive copy is to be retained, called the *retention period*. The retrieval process locates the copies within the archival storage and places them back into a designated system, which might be the active transactional system or a system 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 Disposal

Data Disposal refers to the tools and processes to delete data from a system that is no longer needed and required by law or policy to be retained. 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 processes can create a security risk if they inadvertently leave a way for the disposed data to be retrieved. Data Disposal tools and processes have to be designed to thwart likely threats to recovering the data, 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 tools and processes must also preserve sufficient records to show that the disposal processes have been followed.

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 47):

- Security Info 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 can help tie database interaction to specific individuals, which is becoming more and more important due to increased compliance initiatives.

- Security Policy Infrastructure

  Data access entitlements 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 to ensure this consistency. In addition, data retention policies, disposal policies, and other policies 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 needed actions. It is necessary to show that the responsible people have configured the Data and Information Protection Management systems in accordance with agreed-upon policy and taken responsibility for the actions of the systems that they have 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, additional 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 via 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. While 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, DNS cache poisoning, and so on.

- 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 regarding 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 a wide variety of 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 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 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 only be allowed to see the sales data for the region that he manages.

- Operational Context

  Increasingly, database servers and content repositories are required to be aware of not only the credentials used to access them, but also 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 need to 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 determining 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 life cycle 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.

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.

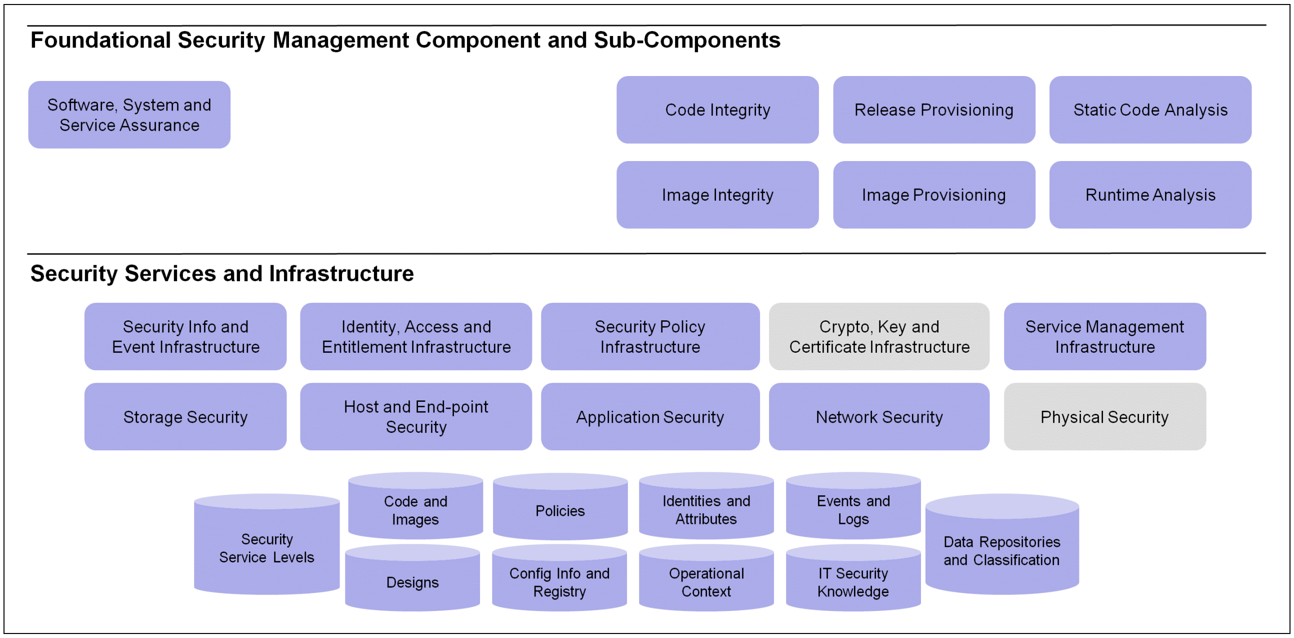

Foundational Security Management Component and Sub-Components
Software, System and Service Assurance
Code Integrity
Release Provisioning
Static Code Analysis
Image Integrity
Image Provisioning
Runtime Analysis
Security Services and Infrastructure
Security Info and Event Infrastructure
Identity, Access and Entitlement Infrastructure
Security Policy Infrastructure
Crypto, Key and Certificate Infrastructure
Service Management Infrastructure
Storage Security
Host and End-point Security
Application Security
Network Security
Physical Security
Security Service Levels
Code and Images
Designs
Policies
Config Info and Registry
Identities and Attributes
Operational Context
Events and Logs
IT Security Knowledge
Data Repositories and Classification

Figure 2-7 Software, System and Service Assurance subcomponents

Software, System and Service Assurance consists of the following subcomponents:

- Code Integrity
- Image Integrity
- Release Provisioning
- Image Provisioning

- Static Code Analysis
- Runtime Analysis

These services are explained in the following sections.

Code Integrity

Code Integrity refers to protecting assets used to build and run application object code to ensure that what is delivered to service management for deployment has not been 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 proper licenses have been 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 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 has not been tampered with after it has been assembled.

Release Provisioning

Secure provisioning ensures that handing over code to release management for installation and configuration of 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.

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.

Static Code Analysis

Static Code Analysis refers to the tools and processes that are usually 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.

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.

While 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 resulting in 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 2.2.6, “Software, System and Service Assurance” on page 52 (depicted as blue-shaded objects in Figure 2-7 on page 52):

- Security Info and Event Infrastructure

  When planning the deployment of an application, the security-relevant events that it might generate need to be planned for in the Security Info 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 into their Security Info 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 regulating 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.

- Service Management Infrastructure

  Assurance activities define deployment and access requirements for applications and images that must be consumed and implemented by the release and deployment processes in the Service Management Infrastructure. Therefore, there needs to be coordination between development and operations to ensure that operations know how to implement the requirements 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 End-point 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 End-point Security to ensure that there are no processes on the host machine intercepting traffic between the application and its clients.

- Application Security

  While 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, SQL injection, and so on.

- Network Security

  Applications have dependencies in the Network Security infrastructure to make certain ports available for remote connections and to ensure the appropriate isolation of network traffic. Certain application-layer attacks can be detected and prevented via 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 backdoors 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 protected by software, server, and security assurance.

- Designs

  The application architecture as 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 a wide variety of Policies that affect software assurance and image integrity. Applications define sets of roles that dictate which features are accessible to which people. These roles need to be mapped to organizational roles by means of 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, 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 have to be mapped to the organizational roles, which requires 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 current 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 extremely important.

- Data Repositories and Classification

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

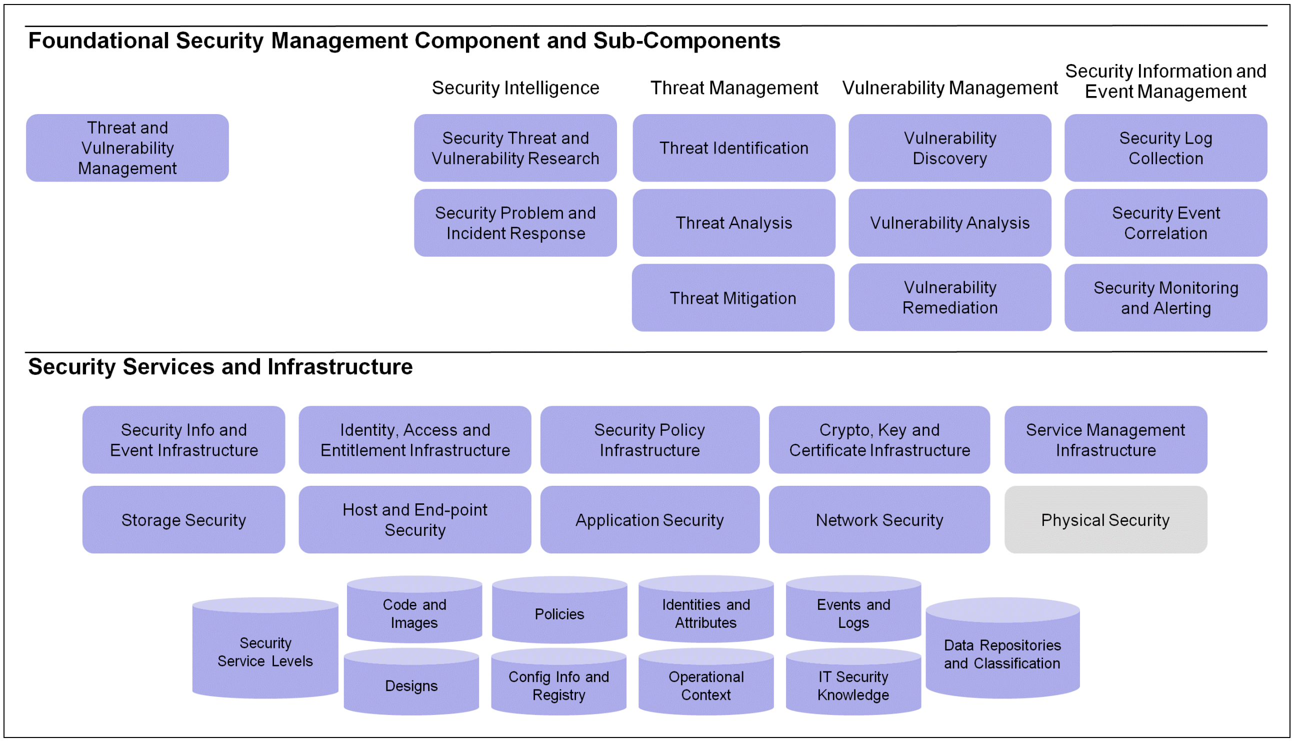

Foundational Security Management Component and Sub-Components
Security Intelligence
Threat Management
Vulnerability Management
Security Information and Event Management
Threat and Vulnerability Management
Security Threat and Vulnerability Research
Security Problem and Incident Response
Threat Identification
Threat Analysis
Threat Mitigation
Vulnerability Discovery
Vulnerability Analysis
Vulnerability Remediation
Security Log Collection
Security Event Correlation
Security Monitoring and Alerting
Security Services and Infrastructure
Security Info and Event Infrastructure
Identity, Access and Entitlement Infrastructure
Security Policy Infrastructure
Crypto, Key and Certificate Infrastructure
Service Management Infrastructure
Storage Security
Host and End-point Security
Application Security
Network Security
Physical Security
Security Service Levels
Code and Images
Designs
Policies
Config Info and Registry
Identities and Attributes
Operational Context
Events and Logs
IT Security Knowledge
Data Repositories and Classification

Figure 2-8 Threat and Vulnerability Management subcomponents

Threat and Vulnerability Management consists of the following subcomponents:

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

These four services 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 sophisiticated 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 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 on 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 Mangement services deal with the identification, understanding, and counterfighting of specific threats that might exist for a given 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. That is, there is no risk.

Threat Identification

Threat Identification embraces activities that help to discover actors and actions in the IT environment that might have a harmful effect on IT assets and the information 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 related to *threat agents*, often called attackers, and their possible *threat actions*, the actual attack, to evaluate the severity of an identified threat, for instance, based on the potential occurrence of an attack due to 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 taken to influence either the threat agents or to manipute the threat actions to reduce the severity of a threat. Usual efforts taken include, for instance, declaring sanctions and disciplinary actions to threat agents upon discovery of their threat actions or even their planning of such threat actions as well as the deployment of measures that negate their actions or identify and deviate them away from a given vulnerability. Threat mitigation can consist of detective controls, such as the deployment of malware detection, intrusion detection, and honeypots.

Vulnerability Management

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

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

Vulnerability Discovery

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

- *Dynamic code analysis* to assess applications for vulnerabilities that might be exploited from an application user's perspective.
- *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 via 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 as well as in the provision of inside knowledge and access rights to simulate different attack scenarios. Providing no inside knowledge is considered a blackbox test, whereas providing the testers with background information about the design and architecture is considered a whitebox test.

Vulnerability Analysis

Vulnerability Analysis covers the actual verification of vulnerabilities by erradication of false positives, and further covers the rating of such vulnerabilities in terms of criticality (for instance, based on their ease of discovery and the complexitity of their exploitability by attackers, as well as on the level of 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 additional preventive security controls such as firewall and intrusion prevention systems with virtual patching capabilities.
- Employ additional 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 has been centrally collected, it can be consolidated and structured as well as combined and correlated to derive more meaningful and human-understandable security information.

Security Log Collection

Security Log Collection 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 in order to have a redundant copy (alongside the logs on the originating systems) in order to retrieve and analyze them during security incidents and problems in case the logs on the originating systems have been compromised.

Security Event Correlation

Security Event Correlation builds upon Security Log Collection. After the log data has been centrally collected, it can be consolidated and structured, standardised, and combined and correlated 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 2.2.7, “Threat and Vulnerability Management” on page 56 (depicted as blue-shaded objects in Figure 2-8 on page 56):

- 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 has the ability to 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 subsequent derivation of security information is essential for all vulnerability-related services within the Threat and Vulnerability Management discipline. The large amount of data 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 back 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 positive* events. A false positive is an event that, from a pure technical security perspective, is considered a threat. For example, a particular event has been 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 will no longer be 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 are dependant 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 utilize the services 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 End-point Security

  Like Storage Security, Host and End-point 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 includes malware scanning and remediation software, host intrusion detection and prevention systems, and security healthchecking software. Besides deploying additional 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 like input revalidation to close known and popular 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 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 they allow you to derive potential attack and testing scenarios for vulnerability discovery and threat analysis services.

- Policies

  Policies are required to 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 executed.

- 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 needs to 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 instance, 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 stored in the configuration management database, security administrators are able to determine either regular behavior or malicious intent and act accordingly.

  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 *revoked*, and there are still activities 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 has to be reviewed by the Threat and Vulnerability Management services to come to a correct conclusion. For example, a discovered suspicious activity, like 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 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 working 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.

> **Restriction:** This section is not intended to be a complete discussion of all IT Service Management domains. We 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.

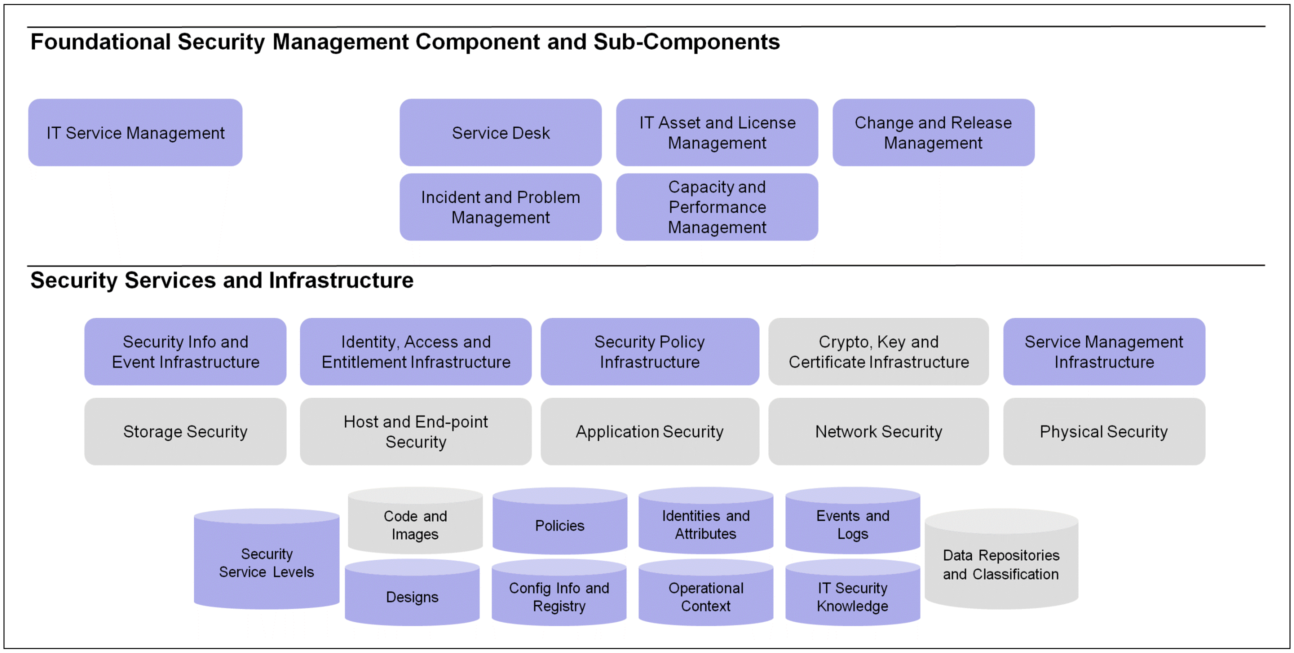

Foundational Security Management Component and Sub-Components
IT Service Management
Service Desk
IT Asset and License Management
Change and Release Management
Incident and Problem Management
Capacity and Performance Management
Security Services and Infrastructure
Security Info and Event Infrastructure
Identity, Access and Entitlement Infrastructure
Security Policy Infrastructure
Crypto, Key and Certificate Infrastructure
Service Management Infrastructure
Storage Security
Host and End-point Security
Application Security
Network Security
Physical Security
Security Service Levels
Code and Images
Designs
Policies
Config Info and Registry
Identities and Attributes
Operational Context
Events and Logs
IT Security Knowledge
Data Repositories and Classification

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 services 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 assists in user charge-back 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 used to restore service from any sort of disruption due to 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 due to its continued significant impact on the level of service or due to the increased efforts that are required to return to normal operations.

From a security perspective, incidents and problems can be classified as security incidents and security problems and will then 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 mostly refers to details like 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 like floor space in a data center. This area is important to security, as the security services and their related infrastructure components deployed in an IT environment can consume a significant amount of resources, and thus can impact performance.

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

Security Services and Infrastructure components

The following Security Services and Infrastructure components are key to effective 2.2.8, “IT Service Management” on page 62 (depicted as blue-shaded objects in Figure 2-9 on page 62):

- 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, which, when confirmed, can become security incidents and security problems and be provided to the Threat and Vulnerability Management services for resolving.

- 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) has to consider potential impact to the Security Service Levels by other service activities when planning and scheduling those.

- 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 effects 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 most 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 as described above.

- 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 actual progress of initiated activities.

- IT Security Knowledge

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

> **Restriction:** This section is not intended to be a complete discussion of all Physical Asset Management domains. We focus 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.

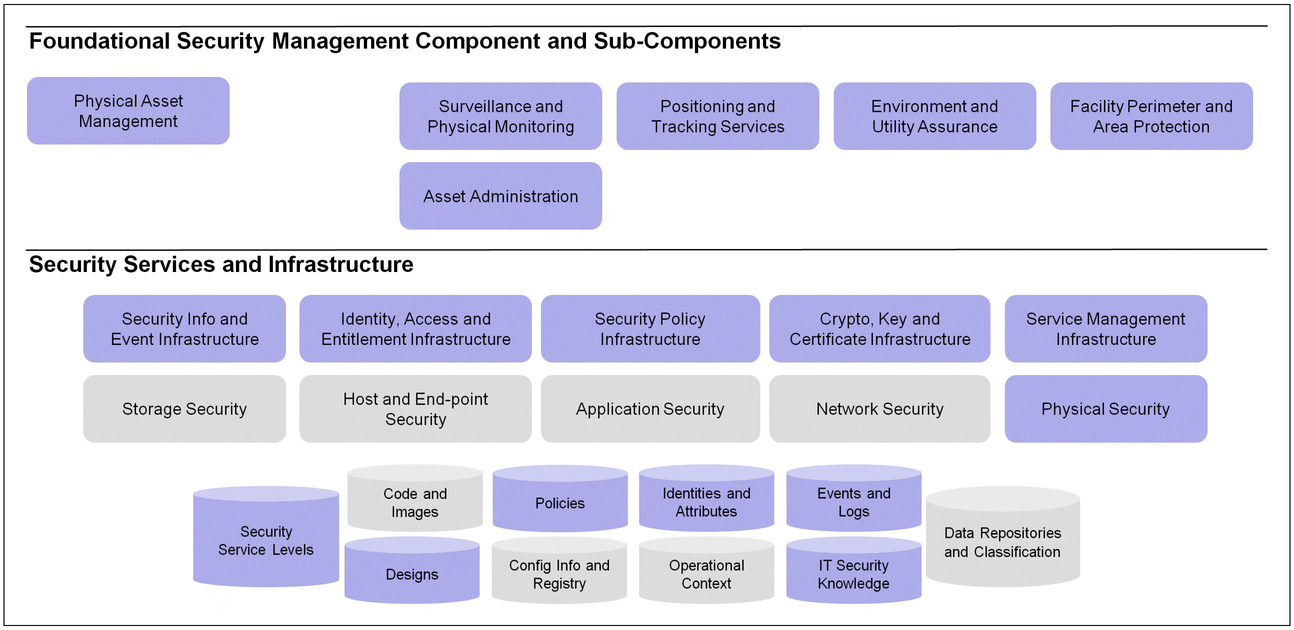

Foundational Security Management Component and Sub-Components
Physical Asset Management
Surveillance and Physical Monitoring
Positioning and Tracking Services
Environment and Utility Assurance
Facility Perimeter and Area Protection
Asset Administration
Security Services and Infrastructure
Security Info and Event Infrastructure
Identity, Access and Entitlement Infrastructure
Security Policy Infrastructure
Crypto, Key and Certificate Infrastructure
Service Management Infrastructure
Storage Security
Host and End-point Security
Application Security
Network Security
Physical Security
Security Service Levels
Code and Images
Designs
Policies
Config Info and Registry
Identities and Attributes
Operational Context
Events and Logs
IT Security Knowledge
Data Repositories and Classification

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 that 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 services 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 triggered by opening doors and gates, breaking or opening windows and hatches, moving objects, or simple discovery of intruders due to motion detection. Surveillance and Physical Monitoring can be performed 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 of time to investigate security-related situations retrospectively.

Environment and Utility Assurance

Environment and Utility Assurance covers the provisioning of electricity and other power utility related supplies and climate controls. Environment and Utility Assurance is an integral 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.

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 need to be protected. This can include short-range and long-range tracking, up to a worldwide scale.

Asset Administration

Asset Administration covers the coordination of activities 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 2.2.9, “Physical Asset Management” on page 65 (depicted as blue-shaded objects in Figure 2-10 on page 66):

- Security Info and Event Infrastructure

  The information about physical environments 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 regarding the access of an application can be correlated with an event representing 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, 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 have to 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, like specific physical controls (barriers, perimeter checkpoints, and so on).

- Designs

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

- Policies

  Policies 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

In this section we explained the IBM Security Blueprint in more detail by discussing the components and subcomponents of the IBM Security Blueprint. We described the subcomponents in detail and related them to the key infrastructure and security services components on which they depend. Next we look more closely at an example business.

3

Business scenario for the People and Identity solution pattern

To illustrate how you can benefit from employing the IBM Security Framework and the IBM Security Blueprint, we discuss a typical business scenario in which we cover the business challenge of reducing password management-related costs.

This scenario is organized into the following sections:

- Business context for reducing password-related costs
- Problem statement and requirements
- IBM Security Framework mapping
- IBM Security Blueprint services

3.1 Business context for reducing password-related costs

Today, users of applications and systems have to manage an increasingly large number of user ID and password combinations. Regulations and policies require these passwords to be complex (containing numbers and non-alphabetic characters, satisfying a minimum length, and so on) and to be changed in ever shorter intervals. This can easily result in lost productivity when users lose or forget their passwords, or do not reset them in time. Resetting passwords is still considered one of the major activities of a help desk function, which can take up to 40% of the call volume with the average cost of a single call as high as $25[1]. If the number of password reset-related calls can be significantly reduced, substantial cost savings might be gained.

Another factor for productivity loss can be the fact that users have to repeatedly provide their credentials when accessing disparate applications or systems. This can also be the case after a user's session has been terminated due to time-out limits.

3.2 Problem statement and requirements

As described in the business context, the objective is to reduce the number of password-related helpdesk calls and to increase the productivity for users by reducing password-related delays. Another implicit requirement is that the involved application and solution systems must maintain their current security levels. Alleviating or removing authentication mechanisms to ease password-related issues is not a solution.

At this point in the process, we can articulate two possible venues for approaching a solution to our problems:

- A single sign-on approach can help users to better handle the multitude of disparate systems requiring an individual authentication process.
- A password reset self-service functionality can reduce help desk calls by empowering users to request a new password on their own.

What are the architectural building blocks and fundamental services required for this solution? How can you make sure to address and involve all the necessary IT systems for your business solutions to gain the most from your investment? Let us take a look at where and how the IBM Security Framework and IBM Security Blueprint can help.

[1] This example can vary greatly between countries and economies.

3.3 IBM Security Framework mapping

After studying the IBM Security Framework in 1.4, "IBM Security Framework" on page 8, and the following discussions about the security domains, we decide to focus on the *People and Identity* domain. Our problem statement is related to users authenticating and gaining access to their applications and maintaining their personal information (here: passwords) (Figure 3-1).

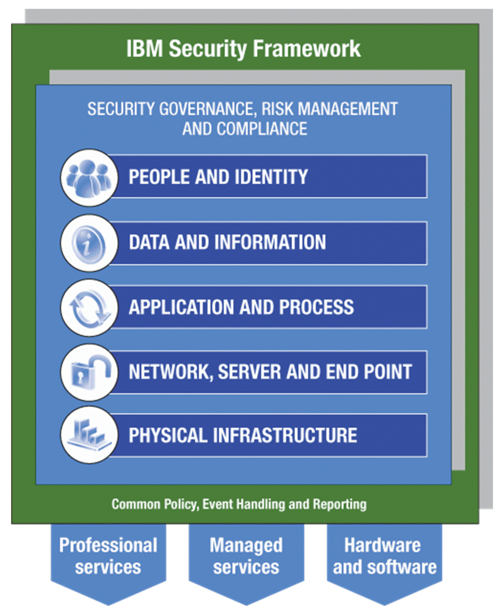


Figure 3-1 IBM Security Framework mapping

Even though there might be an immediate match to the People and Identity domain, it is important to also consider the other IBM Security Framework domains to see whether there is a partial match for reasons of due diligence. In this case, however, the domains of Data and Information, Application and Process, Physical Infrastructure, Security Governance, Risk Management, and Compliance, and Network, Server and Endpoint can be safely left out.

It is a good idea to consistently document your decisions about why you are considering certain aspects and leaving out others to demonstrate due diligence.

3.4 IBM Security Blueprint services

Knowing that we will focus on People and Identity, the next step now is to take a closer look at the blueprint. For each IBM Security Framework domain, we can link the associated components in the IBM Security Blueprint. This is shown in Figure 3-2 on page 72, where the components related to People and Identity are shown with a dark red border.

Three Foundational Security Management services are shown in the middle layer:

- Identity Access and Entitlement Management
- Security Policy Management
- Risk and Compliance Assessment

The *Security Services and Infrastructure* components related to the People and Identity domain are shown in the lower portion of Figure 3-2 on page 72. More details about the

Foundational Security Management and the Security Services and Infrastructure functional components can be found in Chapter 2, “The components of the IBM Security Blueprint” on page 23.

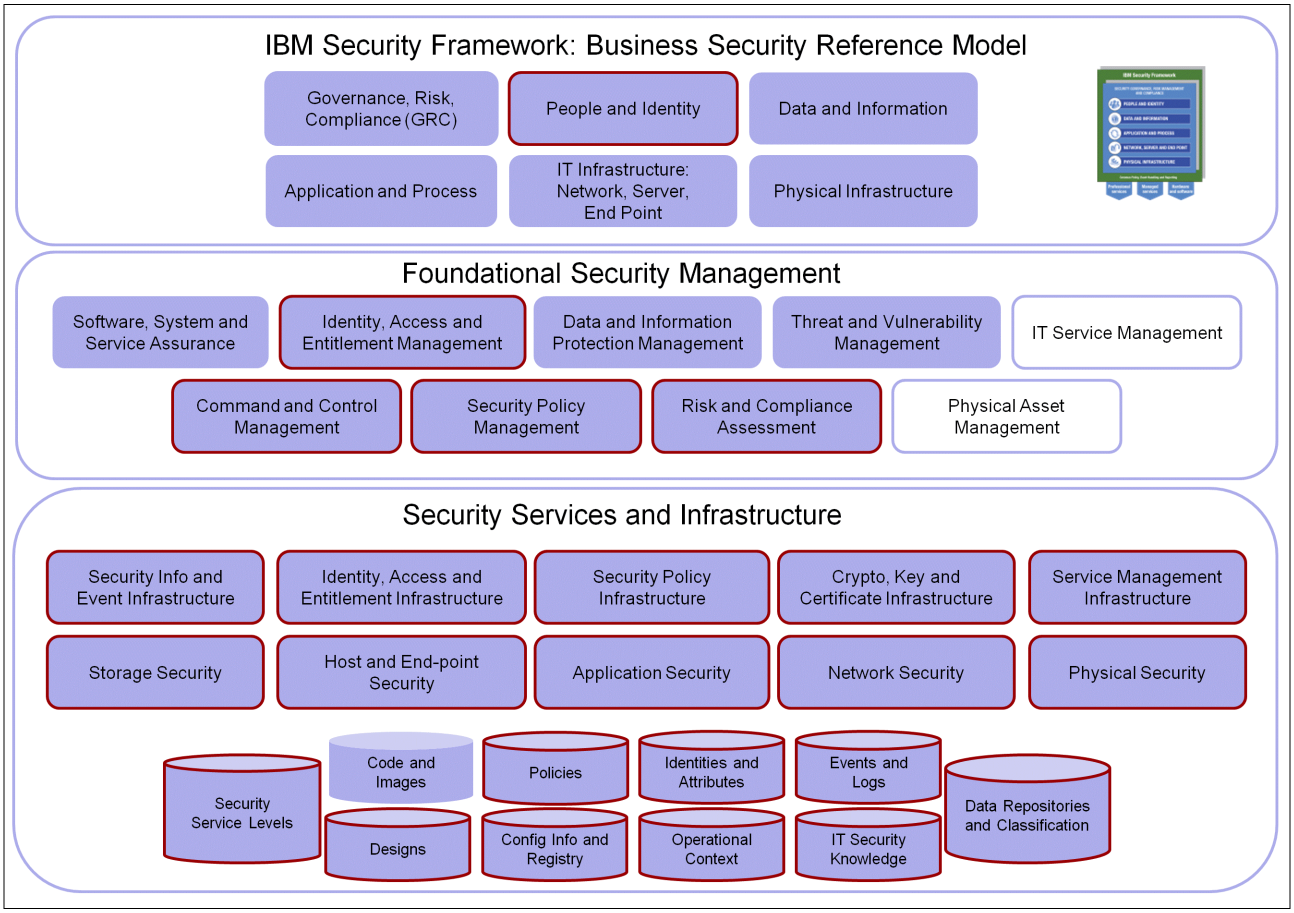

IBM Security Framework: Business Security Reference Model
Governance, Risk, Compliance (GRC)
People and Identity
Data and Information
Application and Process
IT Infrastructure: Network, Server, End Point
Physical Infrastructure
Foundational Security Management
Software, System and Service Assurance
Identity, Access and Entitlement Management
Data and Information Protection Management
Threat and Vulnerability Management
IT Service Management
Command and Control Management
Security Policy Management
Risk and Compliance Assessment
Physical Asset Management
Security Services and Infrastructure
Security Info and Event Infrastructure
Identity, Access and Entitlement Infrastructure
Security Policy Infrastructure
Crypto, Key and Certificate Infrastructure
Service Management Infrastructure
Storage Security
Host and End-point Security
Application Security
Network Security
Physical Security
Security Service Levels
Code and Images
Designs
Policies
Config Info and Registry
Identities and Attributes
Operational Context
Events and Logs
IT Security Knowledge
Data Repositories and Classification

Figure 3-2 IBM Security Blueprint focused on People and Identity

> **Real-life considerations:** In the context of a more typical real-life deployment, you might also want to consider highlighting the *Data and Information Protection Management* service here, because certain tasks within the identity life cycle management might involve collecting personally identifiable information (PII) and issuing secrets, such as passwords or digital certificates, which need to be protected at rest and in transit.
>
> Another Foundational Security Management service that is most likely going to be used in every real-life deployment is the *Command and Control Management* service because every policy, decision, or other related IT task will have to be put into action using these services.
>
> Again, make sure to consistently document your decisions about why you are considering certain aspects and leaving out others to demonstrate due diligence.

As an example, the *Identity, Access and Entitlement Management* component can be further decomposed to reveal more details (Figure 3-3). This more fine-grained level of detail can help you design a thorough architecture to address your requirements. For more details about the identity, access, and entitlement Management services related to roles and identities, access rights, and entitlements, see 2.2.4, “Identity, Access and Entitlement Management” on page 40.

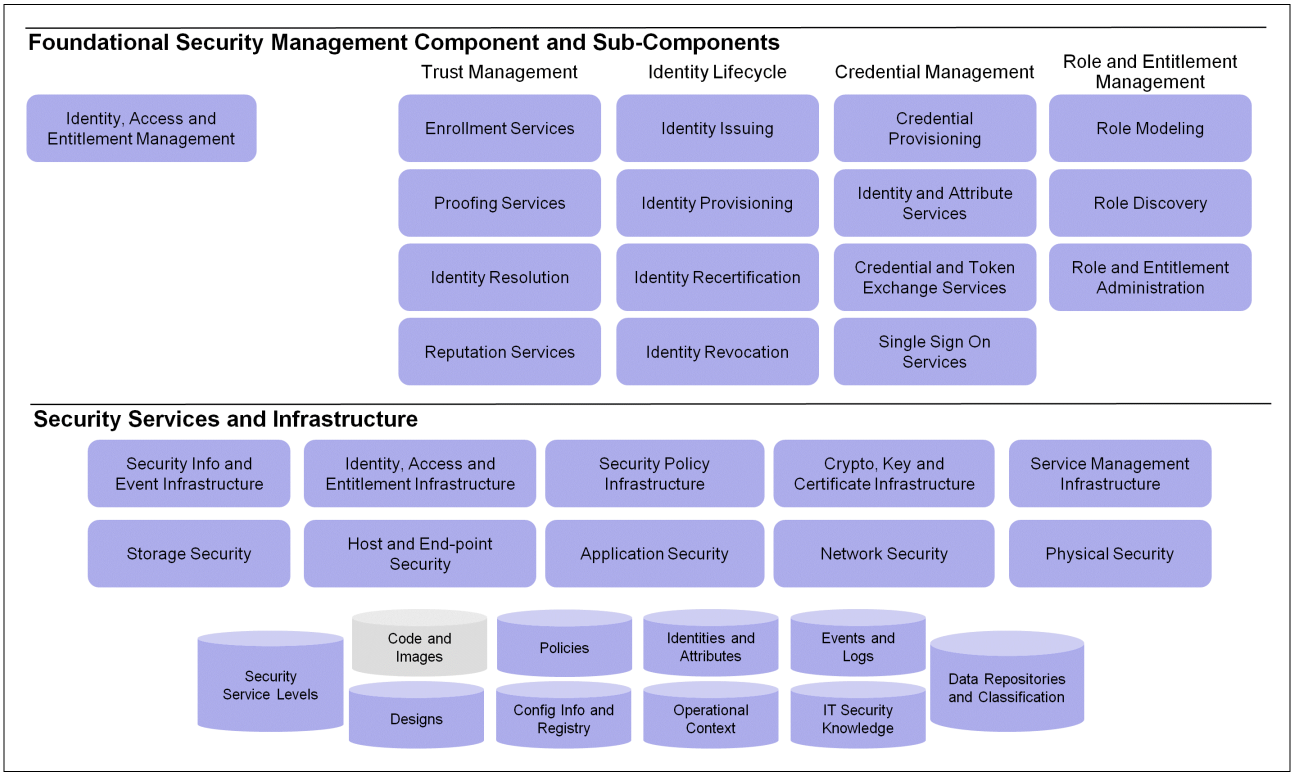

Foundational Security Management Component and Sub-Components
Trust Management
Identity Lifecycle
Credential Management
Role and Entitlement Management
Identity, Access and Entitlement Management
Enrollment Services
Identity Issuing
Credential Provisioning
Role Modeling
Proofing Services
Identity Provisioning
Identity and Attribute Services
Role Discovery
Identity Resolution
Identity Recertification
Credential and Token Exchange Services
Role and Entitlement Administration
Reputation Services
Identity Revocation
Single Sign On Services
Security Services and Infrastructure
Security Info and Event Infrastructure
Identity, Access and Entitlement Infrastructure
Security Policy Infrastructure
Crypto, Key and Certificate Infrastructure
Service Management Infrastructure
Storage Security
Host and End-point Security
Application Security
Network Security
Physical Security
Security Service Levels
Code and Images
Designs
Policies
Config Info and Registry
Identities and Attributes
Operational Context
Events and Logs
IT Security Knowledge
Data Repositories and Classification

Figure 3-3 Identity, Access and Entitlement Management subcomponents

Taking a closer look at the two solution approaches that we defined in 3.2, “Problem statement and requirements” on page 70 (single sign-on and self-service password reset), we can locate the applicable blueprint components in Figure 3-3.

The self-service password reset functionality is part of the *Identity Lifecycle* functional service. They include *Identity Issuing*, *Identity Provisioning*, *Identity Recertification*, and *Identity Revocation*. These represent the major functionality provided by most identity management solutions.

The single sign-on functionality is represented by its own subcomponent, being a part of the set of services around *Credential Management*. Single sign-on is also closely related to the *Identity, Access and Entitlement Infrastructure* component in the *Security Services and Infrastructure* layer because it needs to integrate with existing authentication services.

The next step in this scenario is to further investigate the Security Policy Management and Risk and Compliance Assessment components and their blueprint details.

This decompositional exercise enables you to more consistently define the required architectural building blocks and fundamental services for your organization’s solutions. It can provide you with an overview of how you can ensure to address and involve all the necessary IT systems for your business solutions to gain the most from your investment. Along the way, you will also discover which systems and services can be neglected at this time. Consistently documenting your decisions will help you make the correct decisions and demonstrate due diligence.

The next steps include building a specific solution architecture, design, and implementation. Following this design, along with the architectural principles and industry best practices, leads to an adequate selection of security products and services.

In the following section we take a more general approach of dissecting the People and Identity solution pattern that is not directly tied to this limiting business scenario.

3.5 The People and Identity solution pattern

In this section we discuss how you can use the IBM Security Blueprint material for designing your IT security architecture for the People and Identity domain. This information is also helpful to better understand and to derive IT environment components that are required to establish People and Identity related IT solutions.

3.5.1 Deriving solution patterns for IBM Security Framework security domains

The components of the IBM Security Blueprint can be used to derive overviews for each security domain of the IBM Information Security Framework to outline the respective *Foundational Security Management* services and related *Security Services and Infrastructure* components to address the challenges and generate the values that are summarized under a given security domain. Such an overview is called a *solution pattern* for a security domain.

Solution patterns can be useful to better understand the IT security requirements for a particular business solution. The solution patterns can help you to articulate which *Foundational Security Management* services have to be considered and which *Security Services and Infrastructure* components the services rely on. Solution patterns make it easier to understand the internal relationships between the *Security Services and Infrastructure* components in a specific context given by a security domain. Furthermore, a pattern helps to understand external dependencies on a high, non-technical level and, thus, can be used for many business projects in very early design stages.

As depicted in Figure 3-4 on page 75, the IBM Security Framework security domains can be somewhat mapped to the *Foundational Security Management* services of the IBM Security Blueprint. It is important to understand that this mapping is not a perfect one-to-one match, but rather that the services closest to a given domain provide the main functionality to address the challenges and produce the value associated with a given security domain that the services might require, and in many cases benefit from, in combination with other services.

Also highlighted in Figure 3-4 is the Command and Control Management services because every policy, decision, or other related IT task will have to be put into action using these services.

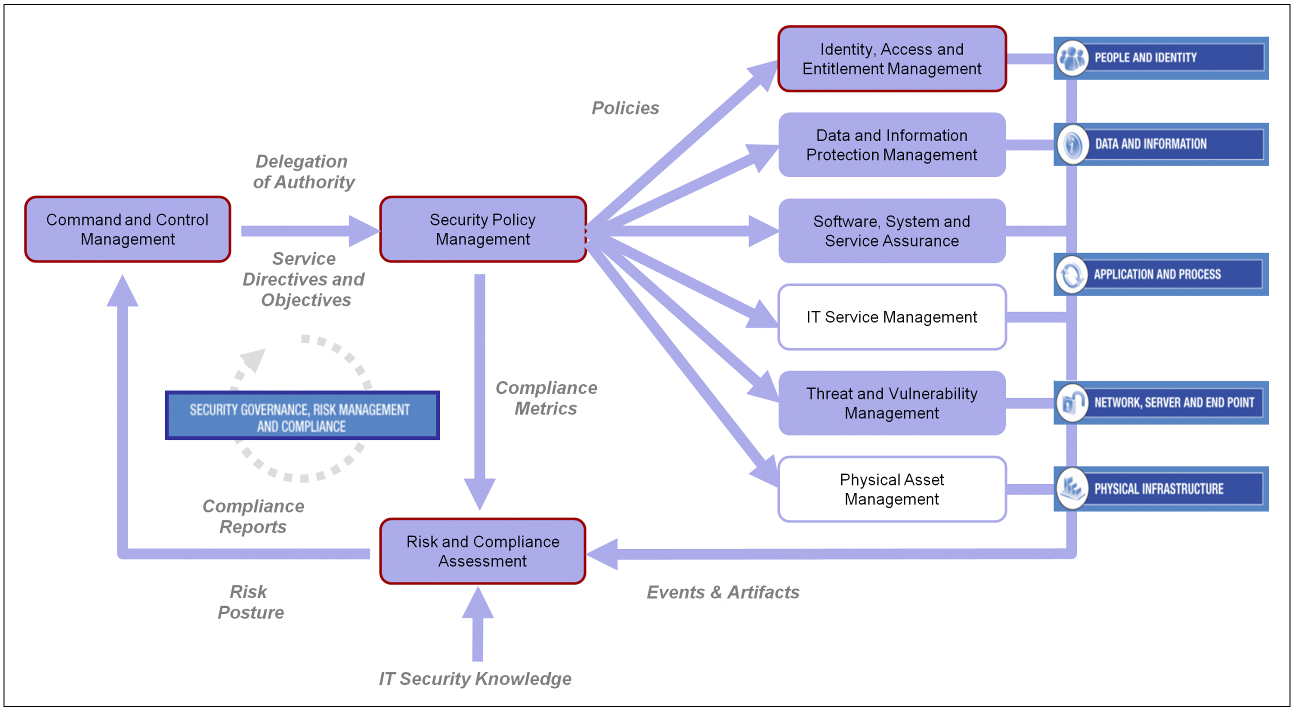

Identity, Access and Entitlement Management
Data and Information Protection Management
Software, System and Service Assurance
IT Service Management
Threat and Vulnerability Management
Physical Asset Management
PEOPLE AND IDENTITY
DATA AND INFORMATION
APPLICATION AND PROCESS
NETWORK, SERVER AND END POINT
PHYSICAL INFRASTRUCTURE
Policies
Delegation of Authority
Command and Control Management
Security Policy Management
Service Directives and Objectives
SECURITY GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE
Compliance Metrics
Compliance Reports
Risk and Compliance Assessment
Risk Posture
Events & Artifacts
IT Security Knowledge

Figure 3-4 Mapping of security domains onto the Foundational Security Management services

In the next sections we derive the solution pattern for the People and Identity domain.

3.5.2 IBM Security Blueprint components for People and Identity solutions

When dealing with any sort of People and Identity challenges from a business perspective, the business context is referenced by the People and Identity security domain of the IBM Security Framework and can be used to better understand and structure the problem on the business level.

From a functional security perspective, People and Identity-related issues can be addressed (and potential values created) primarily by the *Identity, Access and Entitlement Management* services, as discussed in detail in 2.2.4, “Identity, Access and Entitlement Management” on page 40.

However, when taking into account the dependencies as outlined in 2.1, “Foundational Security Management” on page 24, People and Identity solutions also require Security Policy Management services to set policies toward controls for authorized access (for example, the length of passwords or the lockout threshold for unsuccessful login attempts) and to administer these policies throughout their life cycle, as well as to establish them.

Besides Security Policy Management functionality, challenges from the People and Identity domain also have to address a variety of compliance requirements. The challenges can be related to compliance issues resulting from access violations or from required access exceptions due to the dynamics of any successful business environment. Not every new business opportunity can be foreseen, its respective roles and use cases be planned and incorporated into the IT landscape before the opportunity can be pursued, as otherwise many business opportunities might vanish before their benefits can be harvested. Depending on the organization's willingness and capability to handle, mitigate, and accept risk, the Risk and Compliance Assessment service can help to ask the correct questions.

Figure 3-5 highlights the components of the IBM Security Blueprint that have to be examined for every solution within the People and Identity domain. Besides the Foundational Security Management services mentioned previously, the IBM Security Blueprint identifies the corresponding components that the Security Services and Infrastructure need for the domain.

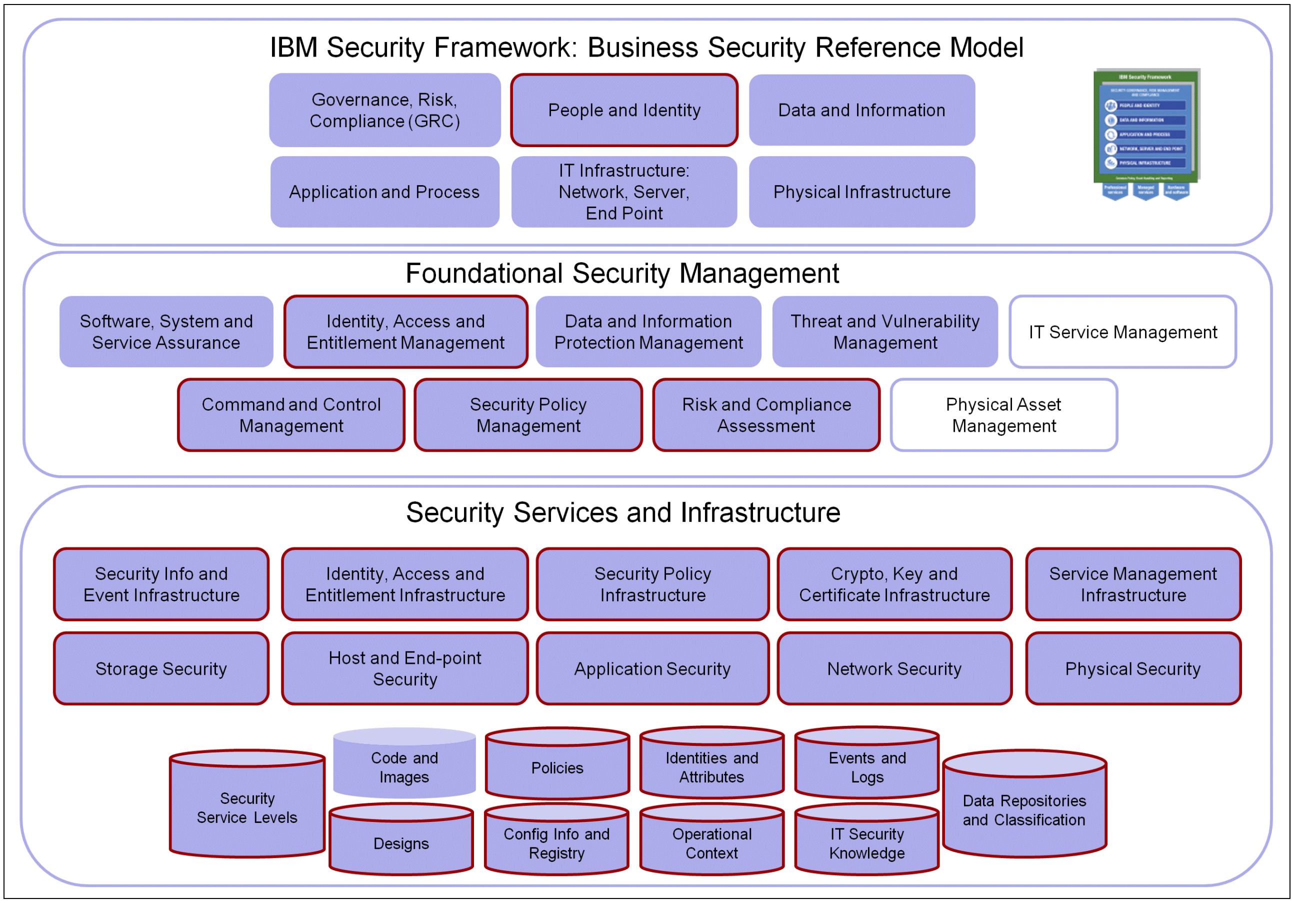

IBM Security Framework: Business Security Reference Model
Governance, Risk, Compliance (GRC)
People and Identity
Data and Information
Application and Process
IT Infrastructure: Network, Server, End Point
Physical Infrastructure
Foundational Security Management
Software, System and Service Assurance
Identity, Access and Entitlement Management
Data and Information Protection Management
Threat and Vulnerability Management
IT Service Management
Command and Control Management
Security Policy Management
Risk and Compliance Assessment
Physical Asset Management
Security Services and Infrastructure
Security Info and Event Infrastructure
Identity, Access and Entitlement Infrastructure
Security Policy Infrastructure
Crypto, Key and Certificate Infrastructure
Service Management Infrastructure
Storage Security
Host and End-point Security
Application Security
Network Security
Physical Security
Security Service Levels
Code and Images
Designs
Policies
Config Info and Registry
Identities and Attributes
Operational Context
Events and Logs
IT Security Knowledge
Data Repositories and Classification

Figure 3-5 IBM Security Blueprint components required for the People and Identity solution pattern

As indicated in Figure 3-5, the functional security diagram for the People and Identity domain indicates that all of the subcomponents of the infrastructure and security services layer except *code and images* are needed for the People and Identity pattern.

The solution pattern allows you to better understand the scope of services to be considered when dealing with People and Identity requirements. The pattern also helps to identity and consider the dependencies that an Identity, Access and Entitlement Infrastructure has to other infrastructures. In other words, the solution pattern clarifies that deploying Identity, Access and Entitlement Management services in isolation will not enable an organization to run the required Foundational Security Management services and, thus, is not sufficient to comprehensively address the requirements and to fully harvest the potential values of the People and Identity security domain.

The solution pattern also serves as a starting point for further, more technical, architecture design. It allows you to identify and map existing components in the IT environment, to identify any missing components, and to help in selecting corresponding software products.

3.6 Conclusion

In this section we provided a business scenario with typical challenges around password management and single sign-on requirements. We discussed how the IBM Security Framework and IBM Security Blueprint can be used to design an IT security architecture solution. We also demonstrated how you can potentially use the decompositional details introduced in Chapter 2, “The components of the IBM Security Blueprint” on page 23, to discuss workflow and dataflow architecture within your solution design.

4

Summary

After we first explored concerns that characterize security requirements of, and threats to, business and information technology (IT) systems, we then identified a number of business drivers that illustrate these concerns, including managing risk and cost, and compliance to business policies and external regulations. We described how security is a major consideration in the way that business and information technology systems are designed, built, operated, and managed.

Because security for information technology can be complex and confounding, IBM created a pair of complementary views to bridge the communication gap between the business and technical perspectives of security. We introduced both the *IBM Security Framework*, which addresses the business view, and the *IBM Security Blueprint*, which addresses the technical view.

In Chapter 2, “The components of the IBM Security Blueprint” on page 23, we explained the IBM Security Blueprint in more detail by discussing the *components* of the IBM Security Blueprint, which can help describe the common security capabilities needed in any IT environment to manage IT security risks. In Chapter 3, “Business scenario for the People and Identity solution pattern” on page 69, we examined a customer scenario that is driven by one major business requirement revolving around the reduction of password management-related costs. We then looked at the IBM Security Framework mapping and used the IBM Security Blueprint services from the subcomponents to describe Foundational Security Management workflows for the involved *people and identity* solution pattern.

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this paper.

IBM Redbooks

You can search for, view, or download Redbooks, Redpapers, Technotes, draft publications and Additional materials, as well as order hardcopy Redbooks publications, at this Web site:

ibm.com/redbooks

Other publications

These publications are also relevant as further information sources:

- A primer about the IBM Security Framework can be found at the following location:

  http://www.ibm.com/security/outlook.html

Online resources

These Web sites are also relevant as further information sources:

- Tap into the interactive IBM Security Community at the following location:

  https://www.ibm.com/communities/service/html/communityview?communityUuid=0629bb73-a904-45b1-86d1-20374d1f1c3e

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security

Redpaper™

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

Connecting business drivers with IT security and risk management disciplines

Employing the IBM Security Framework and the IBM Security Blueprint 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 discussions with business functions and operations exists more than ever.

In this IBM Redpaper publication, we explore concerns that characterize security requirements of, and threats to, business and information technology (IT) systems. We identify a number of the business drivers that illustrate these concerns, including managing risk and cost, and compliance to business policies and external regulations, showing how they can be translated into frameworks to enable enterprise security.

Over the last few decades, industry groups and standards bodies have developed frameworks that serve as a baseline for certain aspects of security, and in this IBM Redpaper publication we discuss two such frameworks, CoBiT and ISO27002.

To help you with your security challenges, IBM has created a bridge to address the communication gap between the business and the 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 solution view.

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

REDP-4528-01