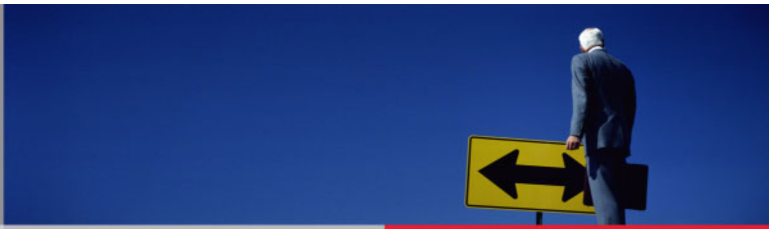
Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security



Redguides

for Business Leaders

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

- 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 real-world business scenarios

Redbooks

Executive overview

In this IBM® Redguide™ publication, we first explore some of the concerns that characterize security requirements of, and threats to, business and information technology (IT) systems. We then identify a number of business drivers that illustrate these concerns, including managing risk and cost, and compliance to business policies and external regulations. We describe how security is a major consideration in the way that business and information technology systems are designed, built, operated, and managed.

In the past decades, industry groups and standards bodies have developed frameworks that serve as a baseline for some aspects of security. We discuss two common frameworks: CoBiT and ISO27002.

Security for information technology can be complex and confounding. Therefore, IBM has created a pair of complementary views to bridge the communication gap between the business and the technical perspectives of security to enable convergence in thought and process. The *IBM Security Framework* addresses the business view, and the *IBM Security Blueprint* addresses the technical view.

The IBM Security Framework was developed to describe security in terms of the business resources that need to be protected, and looks at the different resource domains from a business point of view. It divides IT security into the following six resource 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 the business oriented view of the IBM Security Framework by mapping the domains into a core set of security capabilities and services. These capabilities and services serve as a starting point for design, development, integration, operation, and management of an enterprise IT environment that has security at its core.

With the security domains, capabilities, and services as a backdrop, this guide covers two business scenarios, the first concerning password management related costs, and the second discussing PCI compliance to illustrate how the IBM Security Framework and IBM Security Blueprint can be best used.

This guide is a valuable resource for business leaders, security officers, consultants and architects who wish to understand and implement enterprise security following architectural guidelines.

Business context for IT security

As the pace of globalization picks up, traditional boundaries continue to disappear, melting before the relentless pace of 24x7 communications and trade. In this new global reality, *open for business* can mean that pooling resources and sharing sensitive information among organizations are the *de facto* costs of admission to the global economy. The line between participation and isolation can also mark the line of opportunity and risk. Now more than ever, businesses are relying on computing systems and automation to guard that line: to root out threats, safeguard our intellectual property, and protect our reputation and privacy.

Organizations often adopt a *technology-driven* approach to security. But securing the technology alone does not provide protection for business processes and business assets against business risks. Business leaders can leverage security, risk, and compliance related investments to competitively position their organization and satisfy complex regulatory guidelines.

Organizations often take a *bottom-up* approach to security because security solution vendors often promote this approach to their clients. To close identified security gaps, organizations broaden and bolster their defenses by continually building on top of or adding to their existing security investments. This *technology-centric* methodology often creates an excessively complex and disjointed security infrastructure. It becomes difficult to manage and prone to unseen vulnerability gaps, needlessly escalates IT costs, and eventually fosters unnecessary operational inefficiencies that inhibit business growth rather than enhance it.

Management of business risks requires a *holistic approach* that considers the business goals in concert with the technical requirements and constraints for security. Instead of trying to protect against every conceivable threat, organizations should understand and prioritize the security risk management activities that make the most sense for their organization. By understanding the level of risk tolerance within an organization, the IT team can more easily focus on mitigating risks that the organization cannot afford to neglect. Overemphasizing certain risks can lead to wasted resources and efforts, while underemphasizing others can have disastrous consequences.

Organizations may find it difficult to achieve a strategic, end-to-end security approach that supports business goals, such as driving innovation and reducing organizational costs, as well as operational requirements that address compliance measures and protect against internal and external threats.

Security must not be addressed in isolation from other business activities within the organization. Instead, it has to be viewed from a business perspective—looking at security as a means to protect and enhance business processes.

This 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. Such planning can facilitate the design and building of a *business-driven security blueprint* and strategy that can act as an effective shield of defense for the entire organization that meets business needs and optimize business results.

This security blueprint is influenced by several drivers, so let us take a closer look at those drivers now so that we can better organize and understand the necessary factors.

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 both these influencing factors.

- Business drivers: Business drivers represent constraints placed on by external elements. They can be viewed as business objectives with metrics. The drivers measure value, risk, and economic cost. 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 may vary from industry to industry, from organization to organization in the same industry, and even between 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 represent the key initiatives for security management.

There are several references to the terms *threat*, *threat agent*, and *vulnerability* in the following discussion. According to the International Organization for Standardization (ISO) in their document ISO 15408, Common Criteria:

- Threats are characterized as the potential for abuse of protected assets.
- Threat agents may place a value on assets and seek to abuse or damage assets in a manner contradictory to the interests of the asset owner.
- A vulnerability that may be exploited by threat agents represents a risk to assets and owners.

One of the challenges in developing security management solutions is the dynamic nature and broad scope of threats, threat agents, and vulnerabilities that exist in the environment where managed business systems operate.

> **Note:** You can find ISO 15408 and related documents on the ISO Web site at:
>
> `http://www.iso.org`

Business drivers that influence security

Business drivers that influence security decisions are the first of the two groups of key security initiatives. These represent drivers that may differ from industry to industry, and from application to application within a business. They are considered selective, because a subset of these drivers is applicable depending upon the industry or application.

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 should consistently provide the stakeholders with the expected results.

Security events and incidents may impact the correct and reliable operation of these business processes. It may also affect the underlying IT infrastructure, or upstream and downstream business processes. The consequences of a defective service (not correct or varying results over time) may 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 may 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

Security measures for an IT system are likely to be proportional to the value of the assets found within the system. Asset value relates to the underlying value of the assets transacted in the system. These may be tangible or intangible. For an e-retailer, these are tangible assets. To a financial services company, the asset may be the client information or other data used in transactions of the system. These are the assets behind the system processes.

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 against 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 to 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 upon the structure and terms of the contract, the consequence may lead to financial loss or liability. For example, when security incidents are encountered, the business may 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 may include theft of asset, theft of service, or fraud. Indirect loss may include loss based upon 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, some 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 may 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.

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 may be associated with technology or people.

An example of an internal threat might be a poorly designed system that does not have the appropriate controls. An example of a internal threat agent might be a person who would use their 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 might be a single point 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 might be 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 may result in security exposures to the business. This driver can be divided into two components: 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 (SLAs) can be viewed as a security exposure to business or management processes.

  An example of security exposure for service support is a situation where 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 may 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 with complex architecture is a complex IT environment.

Business environment complexity

Since most businesses rely upon 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 may contribute to the security or insecurity of the IT system.

Audit and traceability

This driver identifies the need for the IT system to support 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 upon 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 system or component design. 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 may be exploited by threats or threat agents as a part of an attack on the IT system, the business, or the management processes. This may include the use of a function within a system in a way to compromise the system, its components, or underlying data. While some define an exploit as both the flaw and the method, we treat them separately because an exploit may 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.

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.

A major challenge in developing and deploying IT security management solutions is apparent with the realization that the business and the IT drivers listed yield a complex set of requirements that impact both the design and operation of the managed business system. The business drivers and the IT drivers listed previously are not mutually exclusive; they are both additive and interdependent.

First, we take a closer look at how these drivers relate to each other. Then we shed a little more light into the risk management discipline, and finally we introduce some common industry approaches that address the holistic approach to enterprise security.

Additive layers of security

Figure 1 provides a simple way to show the inter-relationship of the business (vertical axis) and IT (horizontal axis) drivers. It shows the relationship and any combination of business and IT drivers to the *layers* of protection that would be appropriate for a given solution.

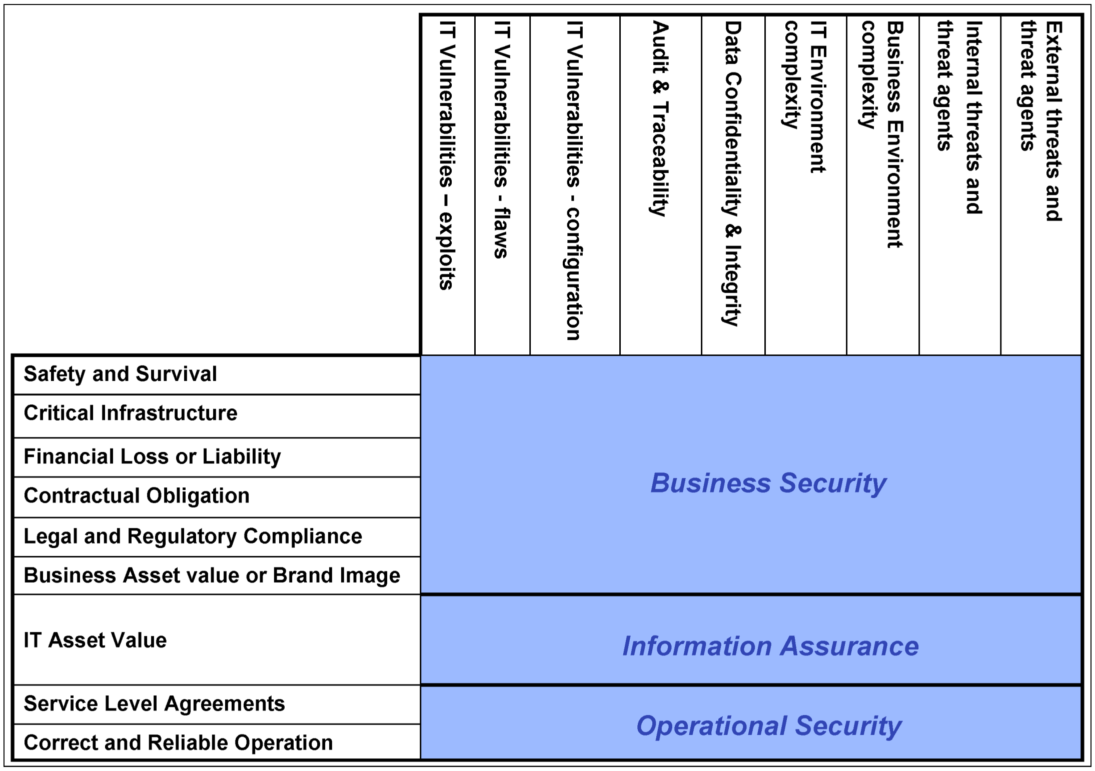

IT Vulnerabilities – exploits
IT Vulnerabilities - flaws
IT Vulnerabilities - configuration
Audit & Traceability
Data Confidentiality & Integrity
IT Environment complexity
Business Environment complexity
Internal threats and threat agents
External threats and threat agents
Safety and Survival
Critical Infrastructure
Financial Loss or Liability
Contractual Obligation
Legal and Regulatory Compliance
Business Asset value or Brand Image
IT Asset Value
Service Level Agreements
Correct and Reliable Operation
Business Security
Information Assurance
Operational Security

Figure 1 Additive layers of IT security management

There are three additive security responses, or layers.

Operational security A mix of reactive and proactive measures that focus on the correct and reliable operation of the infrastructure and managing service levels.

Information assurance Measures that are directed at protecting valued information assets.

Note: Appropriate operational security is assumed for adequate information assurance.

Business security A wide range of measures that address business-specific risks and outcomes.

Note: Appropriate operational security and information assurance is assumed for adequate business security.

Decisions about which layers of IT security management are needed must be made in the light of the analyses of the drivers mentioned in "Drivers that influence security" on page 3. When these drivers are evaluated, they provide the context for use cases. They also lead to the integration of IT security management into our business and IT management model.

Understanding risk management is essential for an effective IT security management system. Let us now take a closer look at the discipline of *risk management*.

Risk management

Every organization faces risk. *Risk analysis* involves the assessment of company assets against what could go wrong, how likely it is to occur, and what damage results from that event. Elements to analyze include:

- Threats: The events, forces, or persons that pose the risk. This could be an event to exploit a vulnerability.
- Probability: The likelihood this threat would occur.
- Damage: The impact of the threat being exploited. This includes loss of service, revenue, potential revenue, and image among customers and peers, and other business specific elements.
- Trade-offs: Evaluating two competing business drivers and evaluating the advantages and disadvantages of each to reach a compromise solution. A common technique to analyze these trade-offs is a *business impact analysis*.

The result of a risk analysis is a collection of risks to the organization. In the next step, *risk mitigation*, an organization determines how to handle those risks. For each risk area, the options are to:

- Reduce: Lower the risk through controls, or technology.
- Transfer: Offload the risk by placing it on some other entity.
- Accept: Decide that the risk is acceptable based on the benefit.
- Ignore: Choose not to reduce, transfer, or accept the risk. This is equivalent to accepting the risk, but without due diligence.

The goal is to reduce the risks identified. A *security policy* can help define mechanisms to better manage risks. This policy involves a combination of process and technology to bring the risk to an acceptable level, as shown in Figure 2 on page 9.

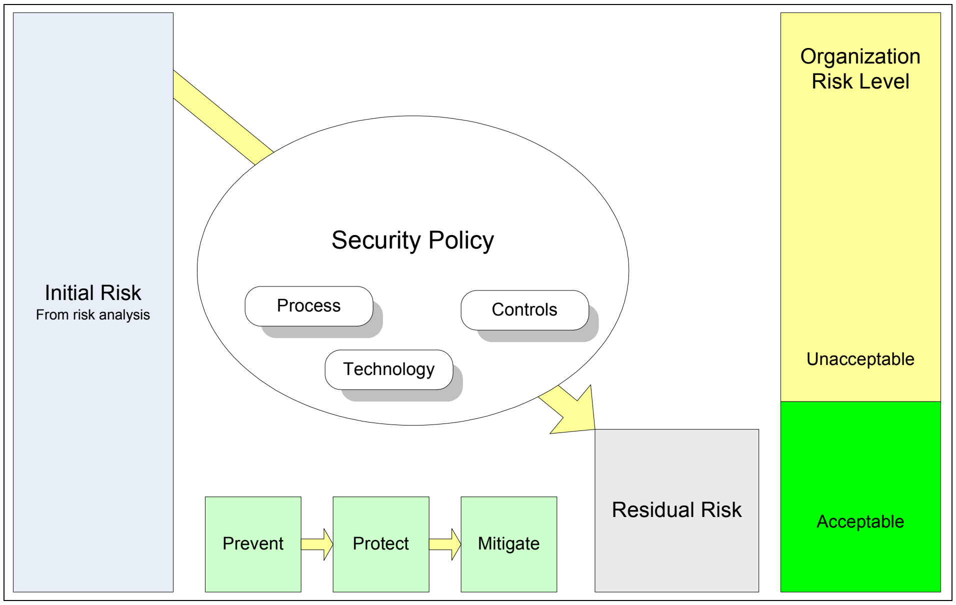


Figure 2 Reducing risk

In Figure 2, the initial risk level is displayed on the left. The security policy provides guidance on controls, processes, and technology to lower the risk. It prevents, protects from, or mitigates the risk, reducing severity. Risk is not eliminated but reduced. An organization establishes what is the acceptable risk level, either quantitatively or qualitatively. This can be through business impact analysis or other techniques to balance risks and benefits. For example, a business may choose to accept a higher risk to accommodate such drivers as time to market and ease of use. The security policy must reduce the residual risk to, or below the level acceptable to the organization for the security policy to be effective. This residual risk can result from an inability to further reduce the risk, or a conscious decision not to invest more resources to do so.

Common industry approaches

The business reasons depicted in "Business drivers that influence security" on page 3 are leading to an evolving number of enterprises who 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] 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`.

Control Objectives for Information and related Technology

Control Objectives for Information and related Technology (CobiT) is a set of best practices (framework) for information technology (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)
- Implementation guide (provides a tool set to implement CobiT)
- IT Assurance guide (explains methods to assess whether control objectives are achieved or not)

The underlying concept of CobiT is that it looks at *business information* that every enterprise needs to support their 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 whole 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, we strongly recommend choosing a top-down approach when implementing CobiT, because business objectives must be clearly defined before the IT strategies can be aligned to it.

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

[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/.

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.

We recommend a step-by-step manner of approaching ISO/IEC 27002:2005. 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.

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

1. Security policy
2. Organization of information security
3. Asset management
4. Human resources security
5. Physical and environmental security
6. Communications and operations management
7. Access control
8. Information systems acquisition, development, and maintenance
9. Information security incident management
10. Business continuity management
11. Compliance

Now it is time for us to introduce the IBM Security Framework (ISF). Its goals are to provide a comprehensive security model based on best practices and open standards that can help you better assess your security posture and efficiently implement an organization-wide security architecture that supports your business growth objectives.

The IBM Security Framework is business problem oriented: it 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.

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 very difficult and is often an afterthought.

IBM created a comprehensive IT security framework, which is shown in Figure 3, that can help ensure that every necessary IT security domain is properly addressed when using a holistic approach to business driven security.

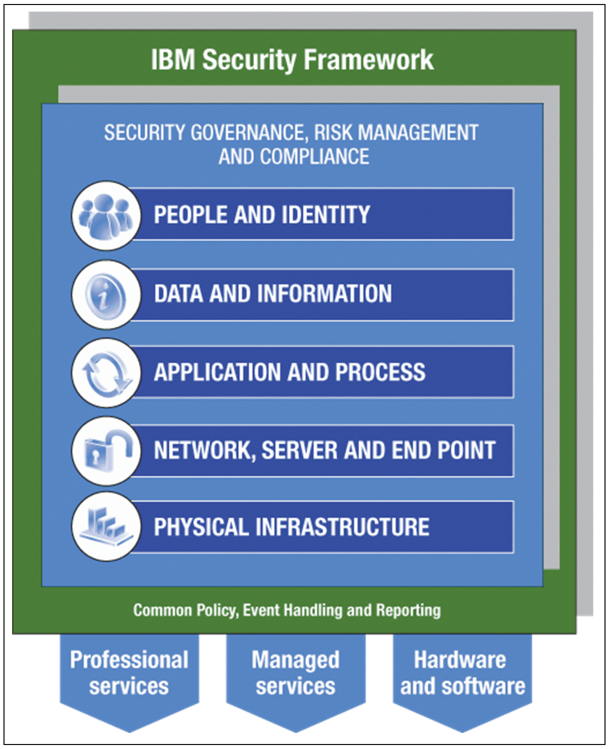


Figure 3 The IBM Security Framework

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

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

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 on how to assure that the right people have access to the right assets at the right time.

- Data and Information

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

- Application and Process

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

- Network, Server, and Endpoint (IT infrastructure)

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

- Physical Infrastructure

  This domain covers aspects on 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.

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.

Security Governance, Risk, and Compliance provides guidance on how identities are managed and how access control should 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), and Physical Infrastructure.

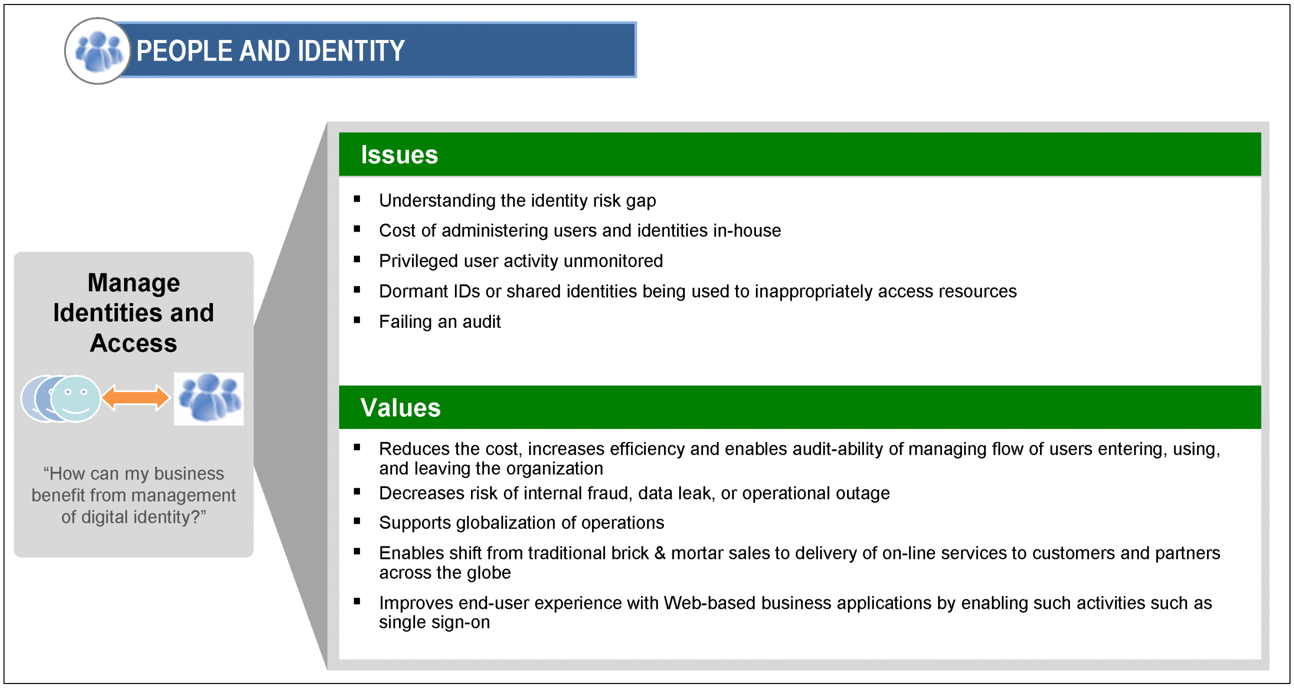
Operationally, people acting in authorized roles in an organization or as part of an extended relationship are granted access to infrastructure, data, information, and services. At the same time, people acting in unauthorized roles are denied access to infrastructure, data, information, and services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

Within an identity system, people may 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 may 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 may contain multiple technology architectures, or multiple identity and access control systems will be required to ensure that users have access to the right 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 4 shows a summary as well as some additional aspects that should 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 4 People and Identity domain

Data and Information

Organizations need to protect both the *raw data* and *contextualized information* that is within its span of control. Security Governance, Risk, and Compliance provides guidance on the value of data and information, as well as on how the risks to data and information should be managed.

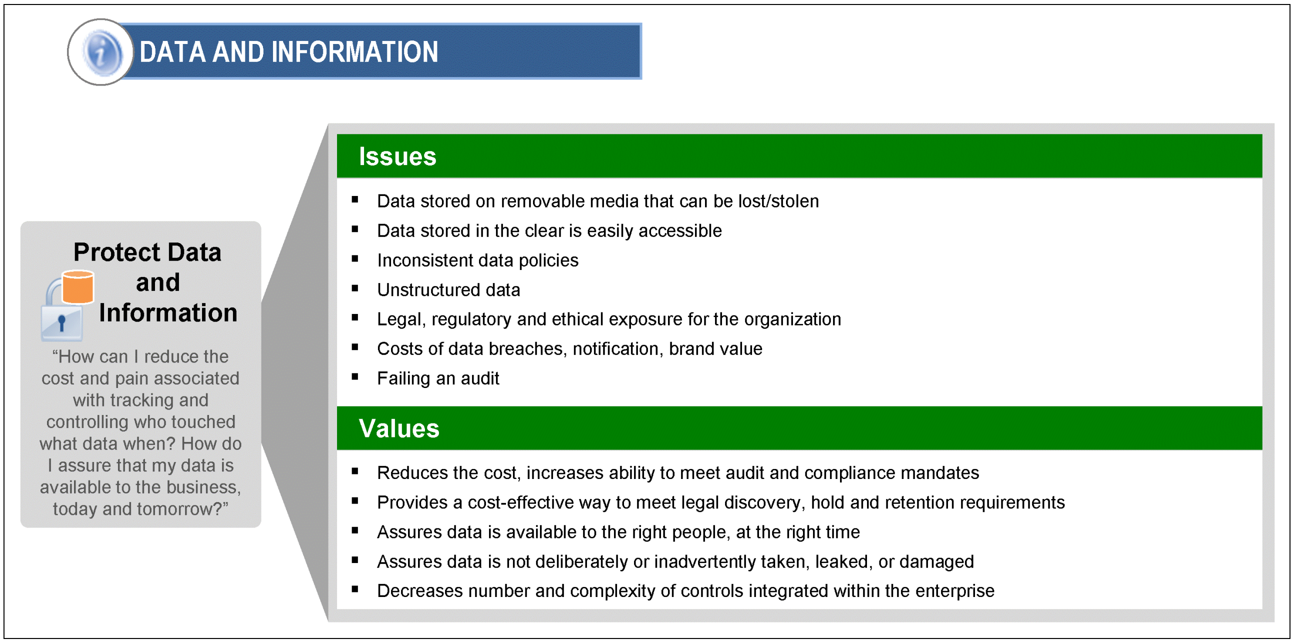
An effective plan for data and information protection includes maintaining a catalog or inventory of these assets, along with attributes, policies, and enforcement mechanisms and services that govern the access, transformation, movement, and disposition of data and information.

This data and information protection plan may 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* may be applied to a wide range of electronically encoded assets. This includes software and firmware, which needs 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 interdependent with 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 5 shows a summary as well as some additional aspects that should 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 5 Data and Information domain

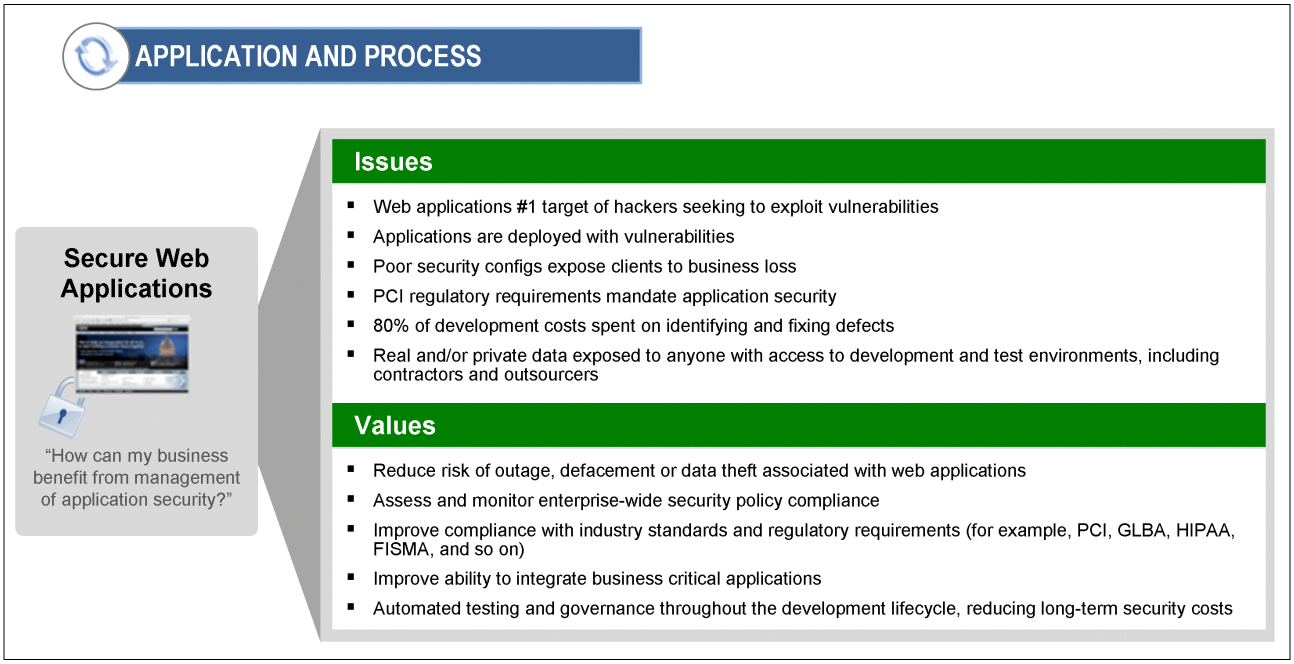
Application and Process

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 an externally facing application, such as a new customer portal, clearly defined security policies and processes are critical to ensure 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 would typically include a combination of capabilities, such as centralized authentication, access and audit policy management, and Web application vulnerability scanning and intrusion prevention.

Figure 6 shows a summary as well as some additional aspects that should 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 6 Application and Process domain

Network, Server, and Endpoint

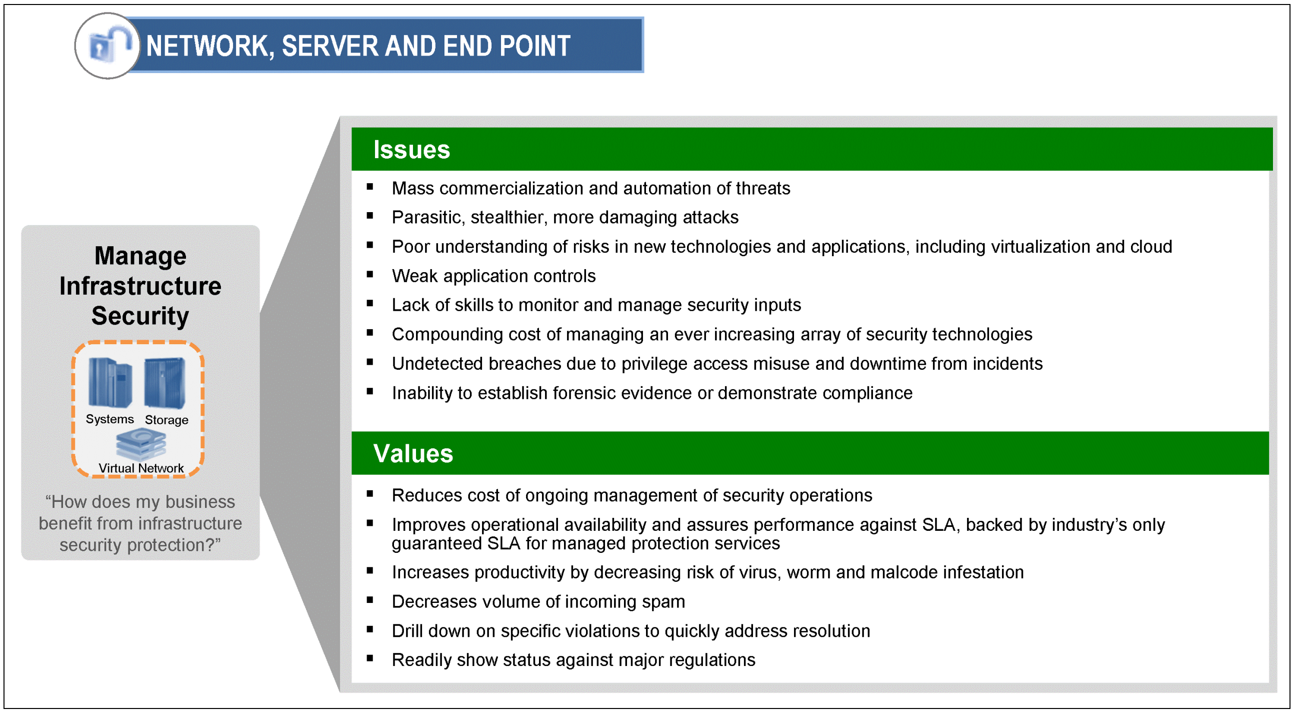
Organizations need to *preemptively* and *proactively monitor* the operation of the business and the IT infrastructure for *threats* and *vulnerabilities* in order to avoid or reduce any breaches.

Security Governance, Risk, and Compliance 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, may 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 are critical to staying ahead of emerging threats that can adversely affect system components and the people and business processes they support. The need to identify and protect the infrastructure against emerging threats have 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.

Enterprises 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 7 shows a summary as well as some additional aspects that should 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 7 Network, Server, and Endpoint domain

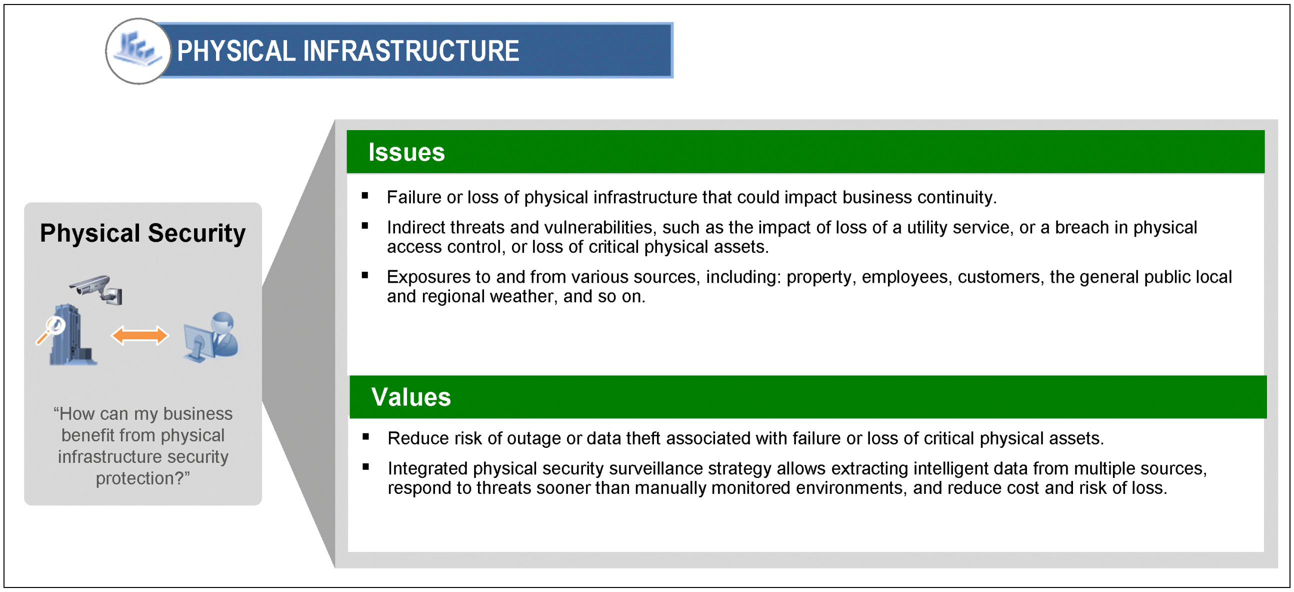
Physical Infrastructure

In order 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, and Compliance provides guidance on the types of risks and the types of plans and responses for physical security.

Protecting an organization's infrastructure may mean taking precautions against a failure or loss of physical infrastructure that could impact business continuity. Protecting an organization's infrastructure may 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 8 shows a summary as well as some additional aspects that should 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 8 Physical Infrastructure domain

After having addressed and mapped the IT security domains into your business solutions, it is time to look at the aspects of creating a more technical security architecture. In the following sections, we discuss the IBM Security Blueprint that will guide you and your IT security professionals to identify the architectural principles that are valid across all domains and environments, as well as the fundamental services within and across the domains and environments.

The IBM Security Blueprint highlights the applicable best practices and IT standards. Building a specific solution requires a specific architecture, design, and implementation; a blueprint helps to create those aspects, but it does not replace them.

IBM Security Blueprint

The IBM Security Framework divides the area of business oriented IT security into several domains. The next step is to break these down into further detail to work towards an architectural framework that can help define and implement your organization’s goals. This architectural framework is 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 business security requirements or areas of concern categorized by the IBM Security Framework. It also defines a common vocabulary to use in further discussions.

In the blueprint, IBM aims to identify architectural principles, that are valid across all domains, and fundamental services within and across the domains. It also highlights applicable best practices and IT standards.

The blueprint has been created based on researching many customer related scenarios focusing on how to build IT solutions based on the IBM Security Framework. The intention of the blueprint is that it can be used as a roadmap to assist in designing and deploying security solutions in your own organization.

Building a specific solution requires a specific architecture, design and implementation—a blueprint can help to create those, *but does not replace them*. Following a blueprint at this point can help find industry best practices and map them to existing security products and services.

IBM has chosen to use a high level service-oriented perspective for the blueprint, based on the IBM Service-Oriented Architecture[5] approach. Services use and refine other services (for example, policy management and access control applies to almost all other services).

To better position and understand the IBM Security Blueprint, look at Figure 9.

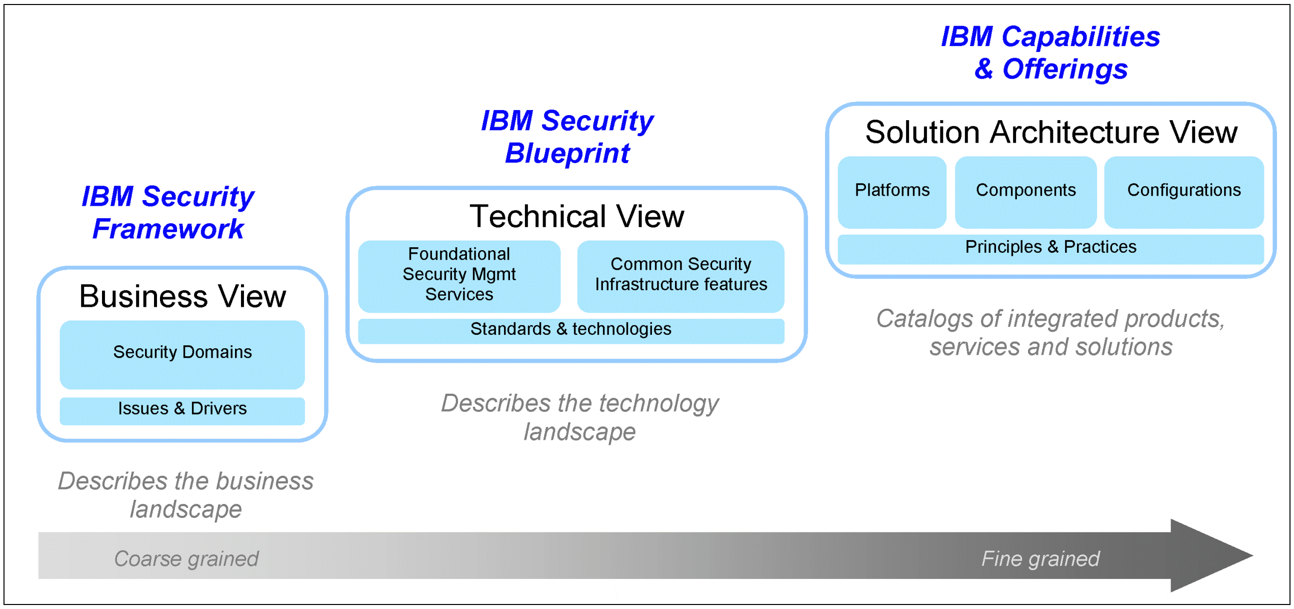

IBM Capabilities & Offerings
Solution Architecture View
Platforms
Components
Configurations
Principles & Practices
Catalogs of integrated products, services and solutions
IBM Security Blueprint
Technical View
Foundational Security Mgmt Services
Common Security Infrastructure features
Standards & technologies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

Figure 9 IBM Security Blueprint positioning

The left portion in this diagram represents the IBM Security Framework, which was covered in "IBM Security Framework" on page 11, and defines the security domains. These represent the business view of security concerns.

The middle portion in Figure 9 represents the IBM Security Blueprint, consisting of three building blocks. The *Foundational Security Management Services* describe the top-level security management services needed to be implemented in order to achieve the required functionality addressed in the IBM Security Framework. These are the layers where the business requirements, as defined in the framework, are converted to top-level IT services to fulfill these requirements. At this point, the threshold has been crossed from pure business related viewpoints to actual IT systems.

The *Common Security Infrastructure features* contain infrastructure elements and services that are used by the top level services in the Foundational Security Management Services. This building block also encompasses existing infrastructure and systems.

Both these IBM Security Blueprint building blocks are founded on open *Standards and technologies*.

Both IBM Security Framework and IBM Security Blueprint can help to better design an IT *Solution Architecture View*, which ultimately describes platforms, components, and configurations following architectural principles and practices.

[5] A comprehensive discussion about the IBM Service-Oriented Architecture can be found in the IBM Redbooks® publication *Understanding SOA Security Design and Implementation*, SG24-7310.

The complete IBM Security Blueprint is shown in Figure 10[6].

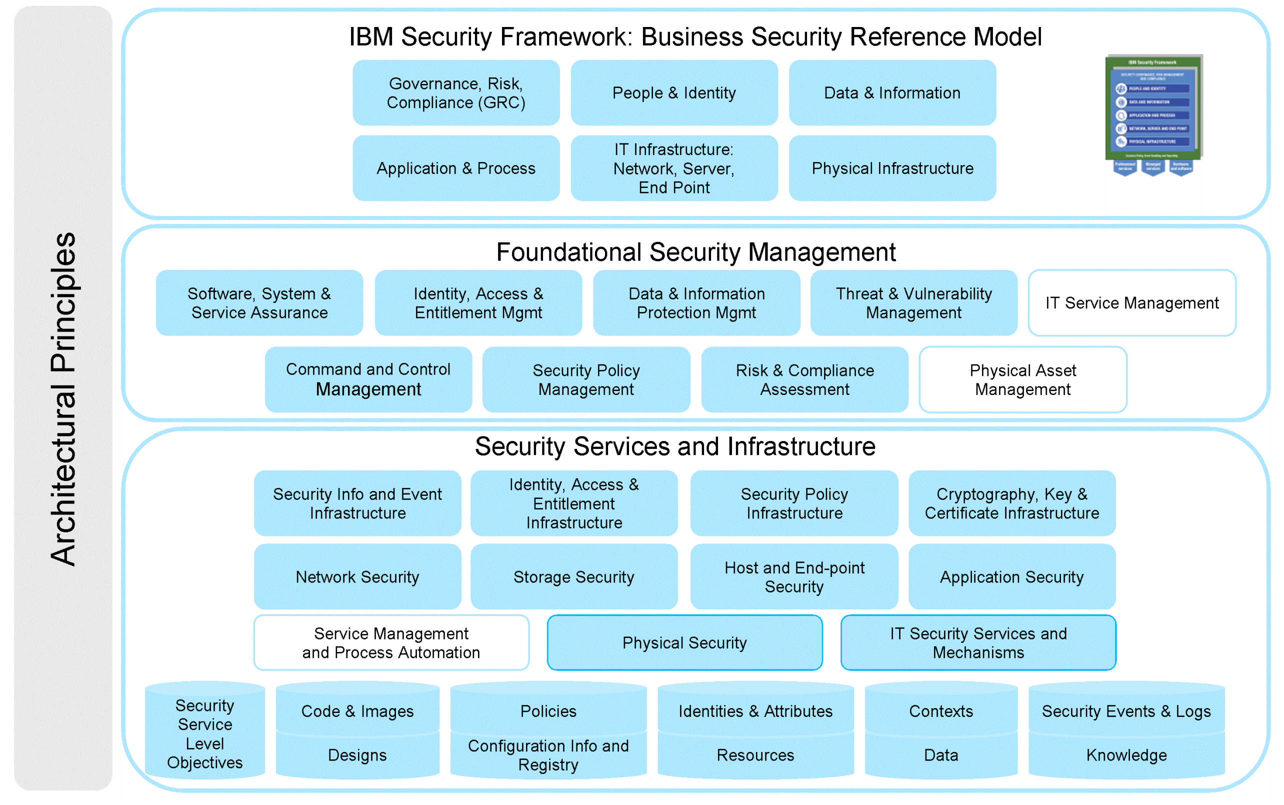

Architectural Principles
IBM Security Framework: Business Security Reference Model
Governance, Risk, Compliance (GRC)
People & Identity
Data & Information
Application & Process
IT Infrastructure: Network, Server, End Point
Physical Infrastructure
Foundational Security Management
Software, System & Service Assurance
Identity, Access & Entitlement Mgmt
Data & Information Protection Mgmt
Threat & Vulnerability Management
IT Service Management
Command and Control Management
Security Policy Management
Risk & Compliance Assessment
Physical Asset Management
Security Services and Infrastructure
Security Info and Event Infrastructure
Identity, Access & Entitlement Infrastructure
Security Policy Infrastructure
Cryptography, Key & Certificate Infrastructure
Network Security
Storage Security
Host and End-point Security
Application Security
Service Management and Process Automation
Physical Security
IT Security Services and Mechanisms
Security Service Level Objectives
Code & Images
Designs
Policies
Configuration Info and Registry
Identities & Attributes
Resources
Contexts
Data
Security Events & Logs
Knowledge

Figure 10 The IBM Security Blueprint

Foundational Security Management

The Foundational Security Management layer contains the top level artifacts, which can be directly mapped to the IBM Security Framework. The sublayers themselves consist of multiple individual and linked services that we describe in more detail in the following IBM Redbooks publications[7].

- *IBM Enterprise Security Architecture for People and Identity*, SG24-7751
- *IBM Enterprise Security Architecture for Governance, Risk and Compliance*, SG24-7750
- *IBM Enterprise Security Architecture for Data and Information*, SG24-7752

The set of foundational security controls form a closed loop management system, as shown in Figure 11 on page 21.

[6] White boxes in this and other diagrams represent services or artifacts that are not solely security related but may be connected with other IT service areas as well.

[7] These IBM Redbooks publications are currently in development and will be published at a later time in 2009.

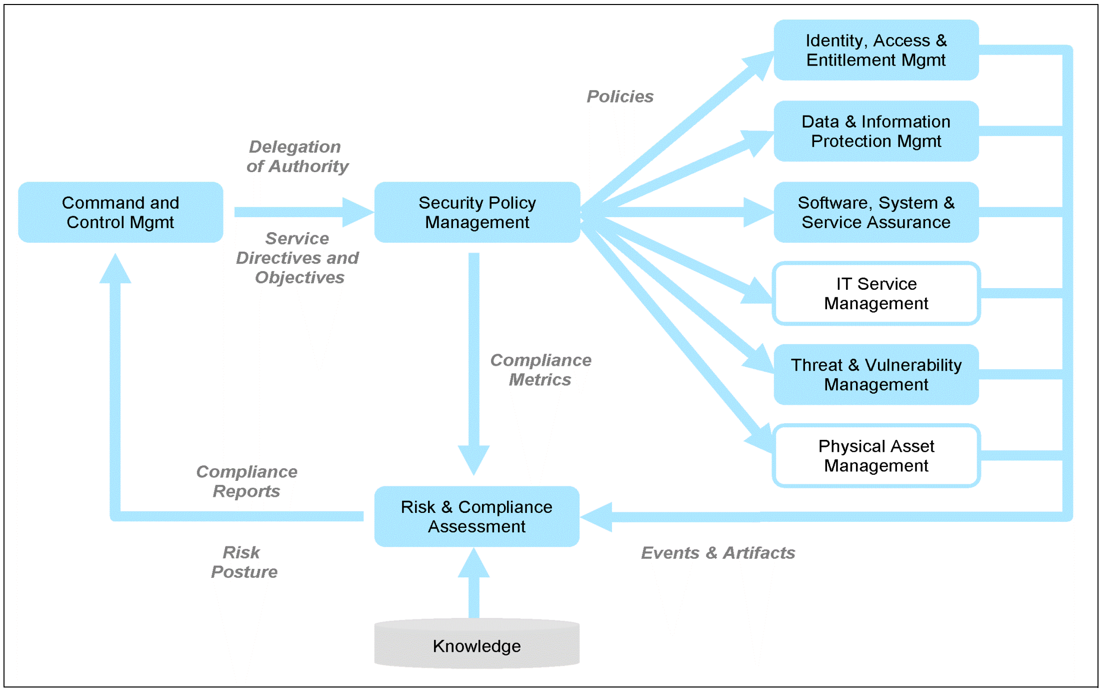

Identity, Access & Entitlement Mgmt
Data & Information Protection Mgmt
Software, System & Service Assurance
IT Service Management
Threat & Vulnerability Management
Physical Asset Management
Policies
Delegation of Authority
Command and Control Mgmt
Security Policy Management
Service Directives and Objectives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

Figure 11 Foundational security controls closed loop

Let us take a closer look at each of the Foundational Security Management controls.

- *Risk and Compliance Assessment* enables the IT organization to collect, analyze, and report security information and security events in order 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* as well as 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, enforcing entry controls, providing for positioning, tracking, and identification of humans and assets, and 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 right identities, at the right time, and for the right purpose. These services can also address 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, and supplier and third-party code validation.
- *IT Service Management* provides the process automation and work flow foundation for security management. In particular, Change & 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.

Security Services and Infrastructure

- *Security Information and Event Management 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 Endpoint 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 OS and system resources to protect against malicious attacks.
- *Application Security* provides the infrastructure for testing, monitoring, and auditing deployed applications.

- *Service Management and Process Automation* consists of the infrastructure services to handle service management processes, such as incident, problem, change, and configuration management. Process automation are generic framework-based services to automate IT actions, including security related activities.
- *Physical Security* are IT infrastructure services 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 may 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.
- *IT Security Services and Mechanisms* provide instrumentation to IT systems for collecting security information and configuration information from IT systems.

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, 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, runtimes, 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 should not be an afterthought in IT solutions, but security policies should 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 should be scalable to handle these events, and audit information must be immutable and non-repudiable.
- Design for regulations.

  Regulations drive many requirements in IT security projects, and regulations change over time. To handle this, it 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 more important. Solutions should 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) shall be provided through a dedicated and shared security infrastructure, enabling consistent monitoring and enforcement. The enforcement itself (through cryptography, through policy enforcement, or through 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 may 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 sections, we cover two business scenario examples to demonstrate how the IBM Security Framework and IBM Security Blueprint can be applied.

Business scenarios

To illustrate how you can benefit from employing the IBM Security Framework and the IBM Security Blueprint, we discuss two separate scenarios. In the first, we cover the business challenge of reducing password management related costs. In the second scenario, we look at the omnipresent Payment Card Industry (PCI) compliance that typically has to cover a broad scope of IT security.

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

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. If the number of password reset related calls can be significantly reduced, substantial cost savings may 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 timeout limits.

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 in order to ease password related issues is clearly 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 in order 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.

IBM Security Framework mapping

After studying “IBM Security Framework” on page 11 and the following discussions around the security domains, we decid to focus on the *People and Identity* domain. Our problem statement is related to users authenticating and gaining access to their applications as well as maintaining their personal information (here: passwords). This is shown in Figure 12.

Even though there may be an immediate match to the People and Identity domain, it is important to also consider the other IBM Security Framework domains to see if there is a partial match for reasons of due diligence. In this case, however, the domains of Data and Information, Applications and Systems, 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 in order to demonstrate due diligence.

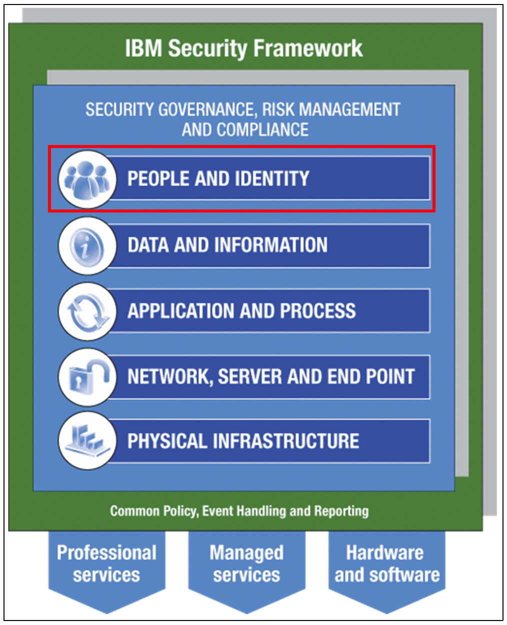


Figure 12 IBM Security Framework mapping

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 artifacts in the IBM Security Blueprint. This is shown in Figure 13 on page 27, where the artifacts related to People and Identity are shown in blue.

Two foundational security management services are shown in the middle layer: *Identity Access and Entitlement Management* and *Security Policy Management*. The password management related issues and tasks fall mostly within the first area, because they are not concerned with security policies. The *Security Services and Infrastructure* artifacts related to the People and Identity domain are shown in the lower portion of the diagram. For simplicity, we will not dissect them any further in this guide.

Note: In the context of a more typical real-life deployment, you may also want to consider highlighting *Data and Information Protection Management* here, because some tasks within the identity lifecycle management may 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. Again, make sure to consistently document your decisions about why you are considering certain aspects and leaving out others in order to demonstrate due diligence.

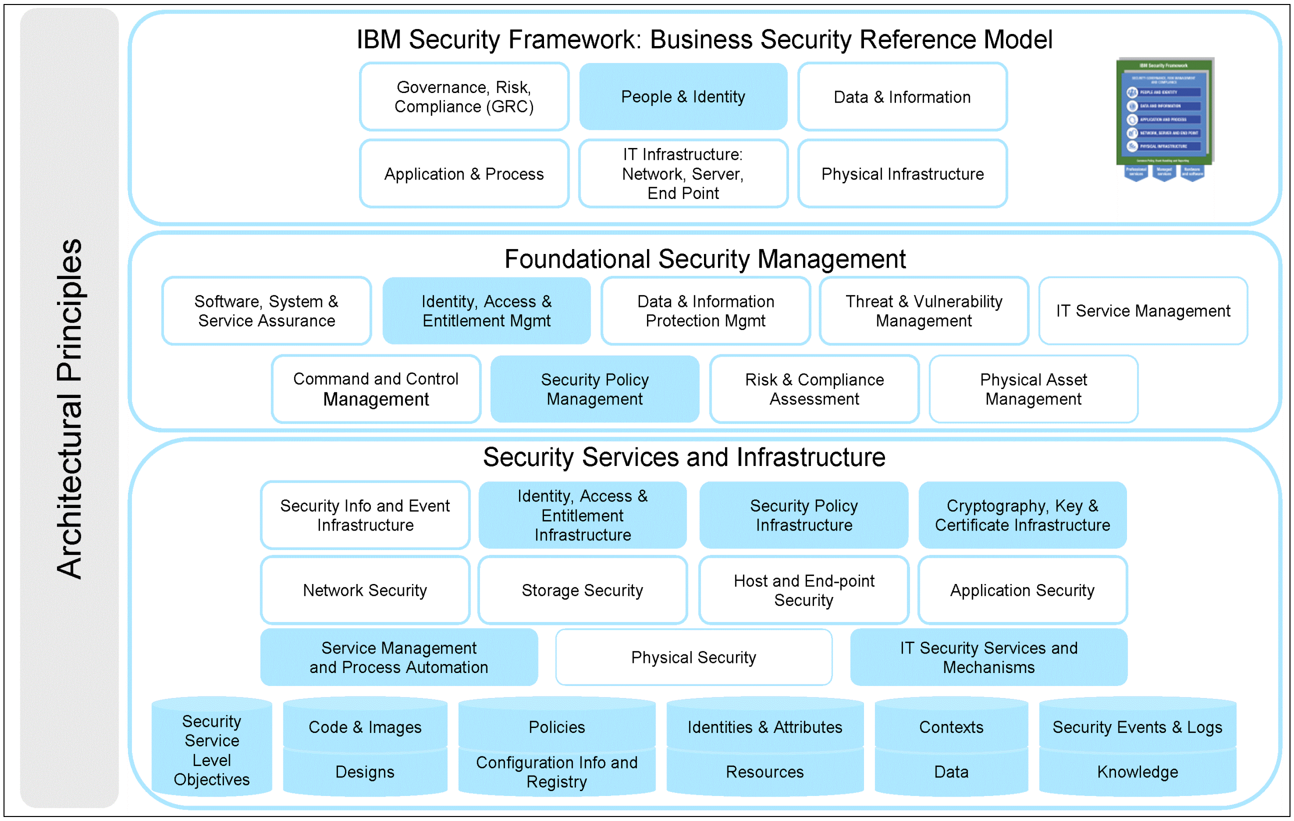

Architectural Principles
IBM Security Framework: Business Security Reference Model
Governance, Risk, Compliance (GRC)
People & Identity
Data & Information
Application & Process
IT Infrastructure: Network, Server, End Point
Physical Infrastructure
Foundational Security Management
Software, System & Service Assurance
Identity, Access & Entitlement Mgmt
Data & Information Protection Mgmt
Threat & Vulnerability Management
IT Service Management
Command and Control Management
Security Policy Management
Risk & Compliance Assessment
Physical Asset Management
Security Services and Infrastructure
Security Info and Event Infrastructure
Identity, Access & Entitlement Infrastructure
Security Policy Infrastructure
Cryptography, Key & Certificate Infrastructure
Network Security
Storage Security
Host and End-point Security
Application Security
Service Management and Process Automation
Physical Security
IT Security Services and Mechanisms
Security Service Level Objectives
Code & Images
Designs
Policies
Configuration Info and Registry
Identities & Attributes
Resources
Contexts
Data
Security Events & Logs
Knowledge

Figure 13 IBM Security Blueprint focused on People and Identity

As an example, the *Identity, Access and Entitlement Management* artifact can be further decomposed to reveal more details, as shown in Figure 14. This more fine-grained level of detail can help you design a thorough architecture to address your requirements.

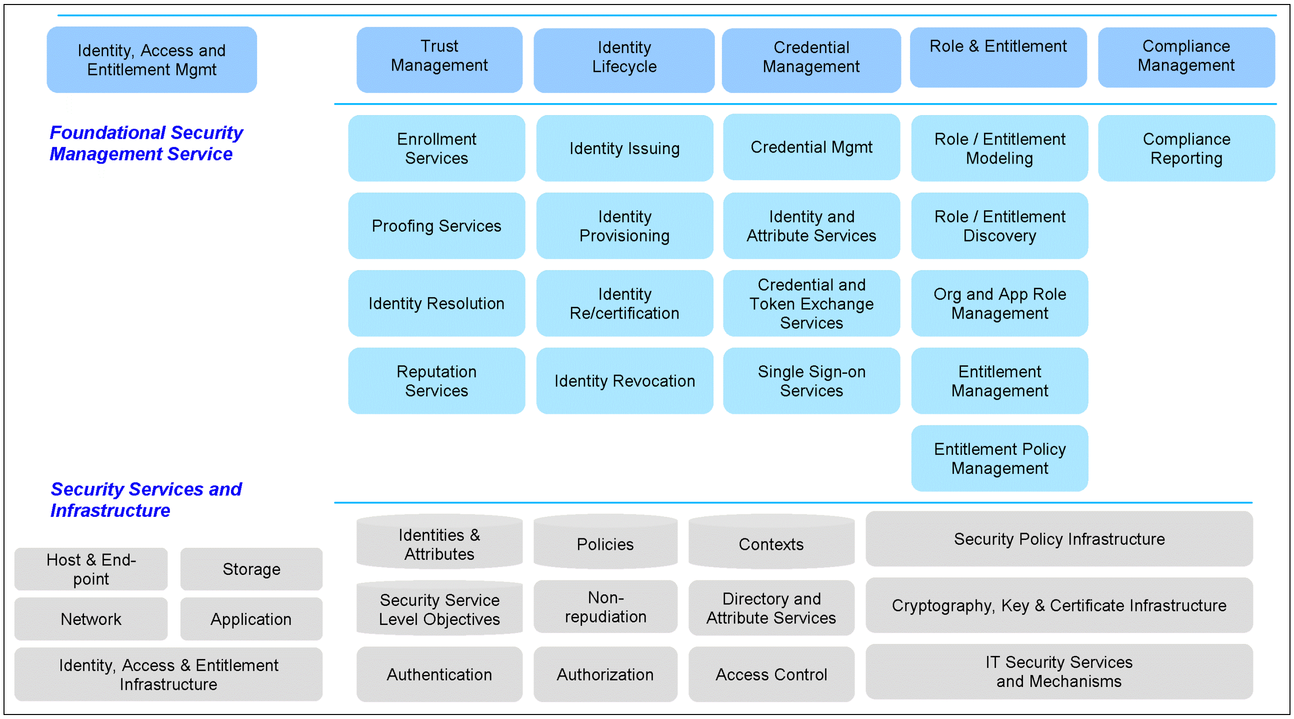

Identity, Access and Entitlement Mgmt
Foundational Security Management Service
Trust Management
Identity Lifecycle
Credential Management
Role & Entitlement
Compliance Management
Enrollment Services
Identity Issuing
Credential Mgmt
Role / Entitlement Modeling
Compliance Reporting
Proofing Services
Identity Provisioning
Identity and Attribute Services
Role / Entitlement Discovery
Identity Resolution
Identity Re/certification
Credential and Token Exchange Services
Org and App Role Management
Reputation Services
Identity Revocation
Single Sign-on Services
Entitlement Management
Entitlement Policy Management
Security Services and Infrastructure
Host & End-point
Storage
Network
Application
Identity, Access & Entitlement Infrastructure
Identities & Attributes
Policies
Contexts
Security Policy Infrastructure
Security Service Level Objectives
Non-repudiation
Directory and Attribute Services
Cryptography, Key & Certificate Infrastructure
Authentication
Authorization
Access Control
IT Security Services and Mechanisms

Figure 14 IBM Security Blueprint details for Identity, Access, and Entitlement Management

Taking a closer look at the two solution approaches we defined in “Problem statement and requirements” on page 25, single sign-on and self-service password reset, we can locate the applicable blueprint artifacts in Figure 14.

The self-service password reset functionality is part of the *Identity Lifecycle services*. 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 service artifact, being a part of the set of services around *Credential Management*. Single sign-on is also closely related to the *Authentication* artifact because it needs to integrate with existing authentication services. Authentication is located in the *Security Services and Infrastructure* layer.

The next step in this scenario would be to have further investigation into the Security Policy Management artifacts and its blueprint details. For simplicity, we do not take this step at this time.

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

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

Now it is time to look at a different example.

Meeting Payment Card Industry Data Security Standard (PCI DSS) compliance needs

This scenario is organized into the following sections:

- Business context for meeting PCI DSS compliance needs
- Problem statement and requirements
- IBM Security Framework mapping
- IBM Security Blueprint services

Business context for meeting PCI DSS compliance needs

Working together, the major payment card providers have developed a set of data security standards and created a council for enforcing them. Although the Payment Card Industry Data Security Standard[8] (PCI DSS) has become a global requirement, many organizations are lagging in compliance. For many companies, regulatory compliance can already be an overwhelming and confusing area to navigate, and the need to comply with the PCI DSS might feel like yet another burden.

However, IBM believes[9] that the PCI standard can instead be seen as an opportunity for many organizations. The standard is so well designed that it can actually serve as the foundation of a risk management strategy going forward.

In this second scenario, we consider a business situation around compliance requirements driven by external regulations. We briefly discuss the PCI DSS standard and how it can be addressed by using the IBM Security Framework and IBM Security Blueprint.

All organizations who transmit, process, or store payment card information must comply with this standard. Compliance is not mandated by the PCI Security Standards Council but by the individual payment card companies.

In our scenario, we discuss PCI compliance from the point of view of a merchant or service provider, that is, a party that accepts payment cards and returns a service to the cardholders.

Problem statement and requirements

The merchant or service provider is required by the payment card industry to comply with the PCI-DSS standard[10]. Depending on the type of merchant or service provider, this can either be achieved by a self-assessment questionnaire, or it needs to be executed by a qualified security assessor.

[8] The PCI Security Standards Council is an open global forum for the ongoing development, enhancement, storage, dissemination, and implementation of security standards for account data protection. You can find more information on their work at https://www.pcisecuritystandards.org/.

[9] In the IBM whitepaper *Profiting from PCI compliance* (December 2007), IBM explores the efficiency gains of building a strategy designed around PCI compliance. This whitepaper can be obtained at ftp://ftp.software.ibm.com/software/tivoli/whitepapers/GTW01773-USEN-00.pdf.

[10] The PCI DSS standard is publicly available, and more information can be found at https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml.

As a quick reference, let us list the basic principles and accompanying requirements around which the specific elements are defined.

- Build and Maintain a Secure Network.

  Requirement 1: Install and maintain a firewall configuration to protect cardholder data.

  Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

- Protect Cardholder Data.

  Requirement 3: Protect stored cardholder data.

  Requirement 4: Encrypt transmission of cardholder data across open, public networks.

- Maintain a Vulnerability Management Program.

  Requirement 5: Use and regularly update antivirus software.

  Requirement 6: Develop and maintain secure systems and applications.

- Implement Strong Access Control Measures.

  Requirement 7: Restrict access to cardholder data by business need-to-know.

  Requirement 8: Assign a unique ID to each person with computer access.

  Requirement 9: Restrict physical access to cardholder data.

- Regularly Monitor and Test Networks.

  Requirement 10: Track and monitor all access to network resources and cardholder data.

  Requirement 11: Regularly test security systems and processes.

- Maintain an Information Security Policy.

  Requirement 12: Maintain a policy that addresses information security.

As you can see from the principles above, PCI DSS is a standard that encompasses a wide area of information security disciplines.

IBM Security Framework mapping

Because meeting PCI DSS compliance is imposed by external regulations, we know we have to closely investigate the Security Governance, Risk Management and Compliance domain, but we must, once more, also consider all the other IBM Security Framework domains. In Figure 15 on page 31, we mark the applicable areas of the IBM Security Framework.

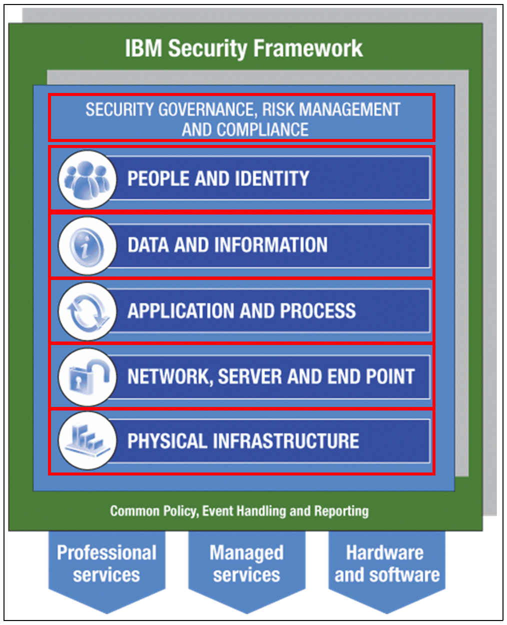


Figure 15   IBM Security Framework mapping

Since PCI DSS is a broadly applicable IT security standard, it comes as no surprise that all the IBM Security Framework domains need to be investigated and documented in regards to the PCI DSS compliance requirement.

In Table 1, we show a mapping of the high level PCI DSS principles to the IBM Security Framework domains.

Table 1   Mapping PCI DSS principles to IBM Security Framework

PCI DSS principle	IBM Security Framework Domain
Build and Maintain a Secure Network.	IT Infrastructure and Network, Server, and Endpoint
Protect Cardholder Data.	Data and Information and Application and Process
Maintain a Vulnerability Management Program.	IT Infrastructure and Network, Server, and Endpoint
Implement Strong Access Control Measures.	People and Identity
Regularly Monitor and Test Networks.	IT Infrastructure and Network, Server, and Endpoint
Maintain an Information Security Policy.	Security Governance, Risk Management, and Compliance

IBM Security Blueprint services

The security principles defined by PCI DSS contain a number of requirements, which in turn consist of more detailed requirements and the required reporting capabilities.

In Table 2, the PCI DSS requirements are listed and mapped to IBM Security Blueprint sublayers. This exercise helps us find all necessary IT security artifacts that have to be investigated more closely.

Table 2 Mapping PCI DSS requirements to IBM Security Blueprint

PCI DSS requirement	Security Blueprint Sublayer
Install and maintain a firewall configuration to protect cardholder data.	► Threat and Vulnerability Management ► Network Security ► Host and Endpoint Security
Do not use vendor supplied defaults for system passwords and other security parameters.	► Software, System and Service Assurance ► Network Security ► Host and Endpoint Security
Protect Stored Cardholders Data.	► Security Policy Management ► Data and Information Protection management ► Cryptography, Key, and Certificate Infrastructure ► Storage Security ► Identity, Access, and Entitlement Management
Encrypt transmission of cardholder data across open, public networks.	► Security Policy Management ► Cryptography, Key, and Certificate Infrastructure ► Network Security
Use and regularly update antivirus software.	► Threat and Vulnerability Management
Develop and maintain secure systems and applications.	► Software, System, and Service Assurance ► Application Security ► Identity, Access, and Entitlement Management ► Data and Information Protection management ► Change and Release Management ► Storage Security ► Threat and Vulnerability Management
Restrict access to cardholder data by business need-to-know.	► Identity, Access, and & Entitlement Management ► Application Security
Assign a unique ID to each person with computer access.	► Identity, Access, and Entitlement Management
Restrict physical access to cardholder data.	► Physical security ► Physical Asset Management
Track and monitor all access to network resources and card data.	► Network Security ► Security Information and Event Infrastructure
Regularly test security systems and processes.	► Network Security ► Threat and Vulnerability Management ► Software, System, and Service Assurance ► Risk and Compliance Assessment ► IT Service Management ► Host and Endpoint Security

PCI DSS requirement	Security Blueprint Sublayer
Maintain an information security policy.	► Risk and Compliance Assessment ► Identity, Access, and Entitlement Management ► Incident Management ► IT Service Management ► Security Policy Management ► Command and Control Management

This concludes our two brief business scenario excursions. We showed you how to begin mapping IBM Security Framework and IBM Security Blueprint artifacts according to individual business and technical requirements.

Summary

In this IBM Redguide publcation, we discussed business as well as IT related drivers that can influence operational security design for an organization. We shed some light into important IT security disciplines like risk management and introduced additive layers of security that were devised from the business and IT related drivers. We also talked about two of the most common industry approaches when it comes to addressing IT security concerns.

Equipped with the core understanding that IT security is a means to support sound business operations, we introduced the IBM Security Framework and the IBM Security Blueprint. The IBM Security Framework and IBM Security Blueprint bridge the gap between how business views security and how IT views security, to consequently enable convergence in thought and process for an organization wide holistic solution.

Both the IBM Security Framework and the IBM Security Blueprint are designed to help build an IT solution architecture view, which can ultimately describe platforms, components, and configurations following architectural principles and practices.

In order to understand the IBM approach to enterprise security, including an introduction and architectural overview of all IBM products in this field, your next step should be to consult IBM Redbooks publications around the IBM Enterprise Security Architecture story, which are listed in “ “Other resources for more information”.

Other resources for more information

To find more information about the IBM Security Framework and IBM Security Blueprint and how they relate to IBM security products, take a look at the following IBM Redbooks publications[11].

- *IBM Enterprise Security Architecture for People and Identity*, SG24-7751
- *IBM Enterprise Security Architecture for Governance, Risk and Compliance*, SG24-7750
- *IBM Enterprise Security Architecture for Data and Information*, SG24-7752

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

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

[11] These IBM Redbooks publications are currently in development and will be published at a later point in 2009. It is IBM’s stated intention to create a set of IBM Redbooks publications that will address all of the IBM Security Framework domains.

Make sure you check out the Gartner hosted document about Securing Cloud Computing, where the IBM Security Framework is being used as well.

http://mediaproducts.gartner.com/gc/webletter/ibm_stg/issue3/article2.html

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

For more information about IBM offerings addressing single sign-on solution, you may want to look at the whitepaper *Addressing single sign-on inside, outside, and between organizations*, December 2008, which can be found at:

ftp://ftp.software.ibm.com/common/ssi/sa/wh/n/tiw14018usen/TIW14018USEN.PDF

More information about IBM offerings geared towards PCI DSS solutions can be found at the following address:

http://www.ibm.com/software/tivoli/governance/security/pci.html

The team that wrote this paper

This IBM Redguide publication was produced by a team of specialists from around the world working at the International Technical Support Organization, Austin Center. It was an part of an effort to create the first set of three IBM Redbooks publications around the IBM Enterprise Security Architecture storyline.

Axel Buecker is a Certified Consulting Software IT Specialist at the International Technical Support Organization, 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 22 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.

David Crowther has 30 years experience in the IT industry, the last 23 working for IBM. During his IBM career, he has worked in technical pre-sales, services, and support, and currently works in IBMs BetaWorks, where he manages early beta programs for Tivoli® Security and Provisioning products. In addition, he runs enablement workshops, provides technical support, and acts as a subject matter expert for new products. He also has wide experience in running beta programs on and supporting products from many of the other IBM brands, including large systems, networking, pervasive, Lotus®, voice, and WebSphere®. He is a Consulting IT Specialist, Chartered IT Professional and Chartered Engineer, and holds a Master's degree in Electrical Sciences from Cambridge University.

Foulques de Valence is a Security and Web IT Architect member of the IBM Systems Lab Services team. He provides consulting services in the USA and worldwide mostly for multinational and Fortune 500 corporations. He focuses on security, SOA, WebSphere products, and IBM System z® infrastructures. Foulques is a co-author of multiple publications about IBM security solutions. He also teaches classes and speaks at conferences about security. Previously he worked as an IT Architect with IBM France, specialized in SOA, J2EE™, and z/OS®. He received a Master’s degree in Computer Science and Engineering from Ensimag in France. He furthered his education at the State University of New York in Buffalo and at Stanford University in California, USA.

Guilherme Monteiro is an IT Security Architect with Companhia de Sistemas, an IBM Business Partner in Brazil, with a strong focus on security solutions. He has been involved with IBM security solutions since 1999, implementing directories, access management, identity management, directory integration, risk management, and developing custom solutions for key Brazilian private companies. His company also has a strong position in Linux® security solutions, with several successful implementations on this platform.

Michel Oosterhof is a Senior IT Specialist with IBM Tivoli Software in the Netherlands. He has 11 years of experience in the IT industry. He holds a Master's of Science degree in Applied Physics from the University of Twente. His main areas of expertise include identity and access management. He is currently working as a Technical Sales Specialist for Tivoli security products.

Andrew Quap is a Software Engineer within the IBM Software Group in Austin, Texas. He has worked with IBM security products for over 10 years and is currently the level 2 tech lead for the Tivoli Federated Identity Manager product and works on the team that supports Tivoli Access Manager, Tivoli Access Manager for OS, Tivoli Security Policy Manager, and the Virtual Member Manager component. He has developed introduction materials for customers for the Managed Beta program. He holds a Bachelor of Science degree in Electrical Computer Engineering from the University of Texas at Austin.

Maria Schuett is a Security Architect with AdminWorks, Inc., an IBM Business Partner in Saint Paul, Minnesota, USA. She has over 15 years of technical experience in information security and technology. She has been involved with IBM Tivoli Security solutions since 2004 and specifically with IBM Tivoli Access Manager for e-business since 2000 by delivering solutions in the state government, health care, and insurance industries. She holds a Bachelor's degree in Computer Science from Eastern Michigan University and an Associate's degree in Engineering from Schoolcraft College. Her areas of expertise include ITIL and Archer SmartSuite® Framework for GRC. She has written, for her clients, whitepapers about infrastructure resilience strategies, including the support of Tivoli Identity and Access Manager with ITIL.

Kai Stockmann is an IT Security Specialist from IBM Germany. He has been working in Security Competency in Germany for five years, where he is the responsible architect for compliance and regulatory programs. In this role, he gained much experience in the security and compliance field, specializing in the areas of IT risk assessment, governance, and compliance management. In addition to this role, Kai is involved in audits and reviews in IMT Germany. He holds a Bachelor's degree in Business Informatics from the University of Stuttgart (Germany) and is CobiT and ITIL certified.

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

Wade Wallace
International Technical Support Organization, Austin Center

Maryann Hondo, Calvin Powers, Dr. Michael Waidner, Jim Whitmore, and the whole IBM Security Architecture Board team
IBM

Become a published author

Join us for a two- to six-week residency program! Help write a book dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You will have the opportunity to team with IBM technical professionals, Business Partners, and Clients.

Your efforts will help increase product acceptance and customer satisfaction. As a bonus, you will develop a network of contacts in IBM development labs, and increase your productivity and marketability.

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 e-mail 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

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.

This document, REDP-4528-00, was created or updated on July 22, 2009.

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®
Lotus®
Redbooks®
Redbooks (logo) ®
Redguide™
SmartSuite®
System z®
Tivoli®
WebSphere®
z/OS®

The following terms are trademarks of other companies:

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.

J2EE, and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

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

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