University of San Diego


# SABSA - Intergalactic Banking and Financial Services, Inc.

*Prepared for*

Intergalactic Banking and Financial Services, Inc.

6/21/2020

*Prepared by*

**Alexandre Fernandes Costa**

alexandrecosta@sandiego.edu


University
of San Diego


# Revision and Signoff Sheet

## Document Record

| Date | Author | Version | Change Reference |
|---|---|---|---|
| 06/03/2019 | Alexandre Fernandes Costa | 1.0 | Initial Document Structure |
| 07/07/2019 | Alexandre Fernandes Costa | 1.1 | Document Structure Set/Content Set |
| | | | |


# Table of Contents


***Dedicated to Vanessa Patricio de Camargo Costa for the support on this new endeavor***


# 1 Executive Summary

Cybersecurity is all about protecting business goals and assets. It means providing a set of business controls that are matched to business needs, which in turn are derived from an assessment and analysis of business risks, for this assignment the main deliverables will be based on the SABSA Framework.

In its best possible light, cybersecurity should be enabling business by reducing risks to acceptable levels and thus allowing business and partners to make use of new technologies for greater commercial advantage.

Cybersecurity can also be a means to add value to the core product by enabling information services that are essential to the enhancement of the product itself or to the operational support of the product in the field.

Secure information services can empower internal business partners and external customers, enabling them to do business more easily and securely, and providing them with enhanced services that will have competitive value.

Cybersecurity in business information systems also protects and leverages the trust that exists between business partners, allowing them to establish relationships and to do business in new ways using new technologies.

Cybersecurity architecture is the art and science of designing and supervising the construction of business systems, usually business information systems, which are: hardened against danger, damage; planned for resiliency; able to be relied upon; and hardened against attack threat actors ranging from script kiddies to nation states.

Therefore, cybersecurity architecture is required to create a plan and design of business information systems so that the organization can meet its goals and protect its assets.

There are many open enterprise architecture frameworks, such as:

- SABSA framework and methodology
- The U.S. Department of Defense (DoD) Architecture Framework (DoDAF)


- Extended Enterprise Architecture Framework (E2AF) from the Institute for Enterprise Architecture Developments.
- Federal Enterprise Architecture of the United States Government (FEA)
- Capgemini's Integrated Architecture Framework
- The UK Ministry of Defense (MOD) Architecture Framework (MODAF)
- NIH Enterprise Architecture Framework
- Open Security Architecture
- Information Assurance Enterprise Architectural Framework (IAEAF)
- Service-Oriented Modeling Framework (SOMF)
- The Open Group Architecture Framework (TOGAF)
- Zachman Framework

As you detail the cybersecurity architecture, consider the following success criteria:

- Why is architecture required?
- The architecture is done for a specific stakeholder – make sure you understand and document who that is.
- The architecture maps every component to a set of requirements/constraints.
- The architecture provides the framework that breaks complexity into simplicity.
- A picture is not an architecture – architecture are decisions (why we chose one component vs. another).
- The architecture must document the decisions.
- The architecture must look for strategic implications and value.
- The architecture documents a “technical strategy for the business”.


# 2 Introduction

## 2.1 Background

Intergalactic Banking and Financial Services is a global financial services institution of over 100,000 employees, offering retail and wholesale banking services to customers in over 60 countries.

The Bank operates over 10,000 branches offers a full range of banking services including payment systems, savings, investment advice, and secured and unsecured lending.

While the Bank's position and health are currently secure, numerous trends will impact the Bank's profitability and stability in coming years. The increased digitization of banking is changing the relationship between customers and financial institutions of all types and sizes. Technology continues to reduce the barriers to entry into financial services, and new entrants in this industry bring with them new business models which give them significant advantages over incumbents.

The increased reliance on technology for critical banking services also increases the risk of cybercrime and financial fraud.

The Bank's leadership has recognized these risks and others as drivers for change.

The Bank has performed an internal review and has developed a "bank of the future" strategy which should help the Bank maintain its strong performance in this changing banking landscape.

This business strategy focuses on four key strategic priorities:

- Earn the customer relationship every day with a great experience
- Improve the Bank's use of data insights to understand and anticipate customer needs
- Increase the pace of innovation to anticipate and meet future customer needs and wants


- Develop new services and business models to make Intergalactic Banking and Financial Services the preferred bank of the future for new customers as well as existing ones

This document details the cybersecurity architecture which supports Intergalactic Banking and Financial Services business goals and priorities.

## 2.2 Identified Control Objectives

A cybersecurity strategy was recently developed which identified core security initiatives supporting the Bank's four key strategic priorities. These major security initiatives are important for the organization since they have direct traceability to the Intergalactic Banking and Financial Services business drivers for their digital transformation.

This business strategy focused on four key strategic priorities:

1. Earn the customer relationship every day with a great experience
2. Improve the Bank's use of data insights to understand and anticipate customer needs
3. Increase the pace of innovation to anticipate and meet future customer needs and wants
4. Develop new services and business models to make Intergalactic Banking and Financial Services the preferred bank of the future for new customers as well as existing ones

After taking the strategic priorities through a risk management process, it drove these main control objectives:

1. Secure the Bank's mobile service infrastructure and client apps and protect the Bank's customers' data, no matter where it travels or resides, while making security seamless to the customer.
2. Ensure the Bank's systems provide rich data for investigations.


3. Leverage additional technologies to decrease the total cost of providing secure services to the Bank's business and personal customers.
4. Invest in Bank staff to ensure that new technologies are adopted securely and that they are equipped to respond to security events promptly and with context.

## 2.3 Identifying the Business Attributes

A cybersecurity strategy developed which identified core security initiatives supporting the Bank's four key strategic priorities and business attributes will be aligned to that.

The business attribute profile describes the risks of business failure and what success looks like in terms of risk mitigation.

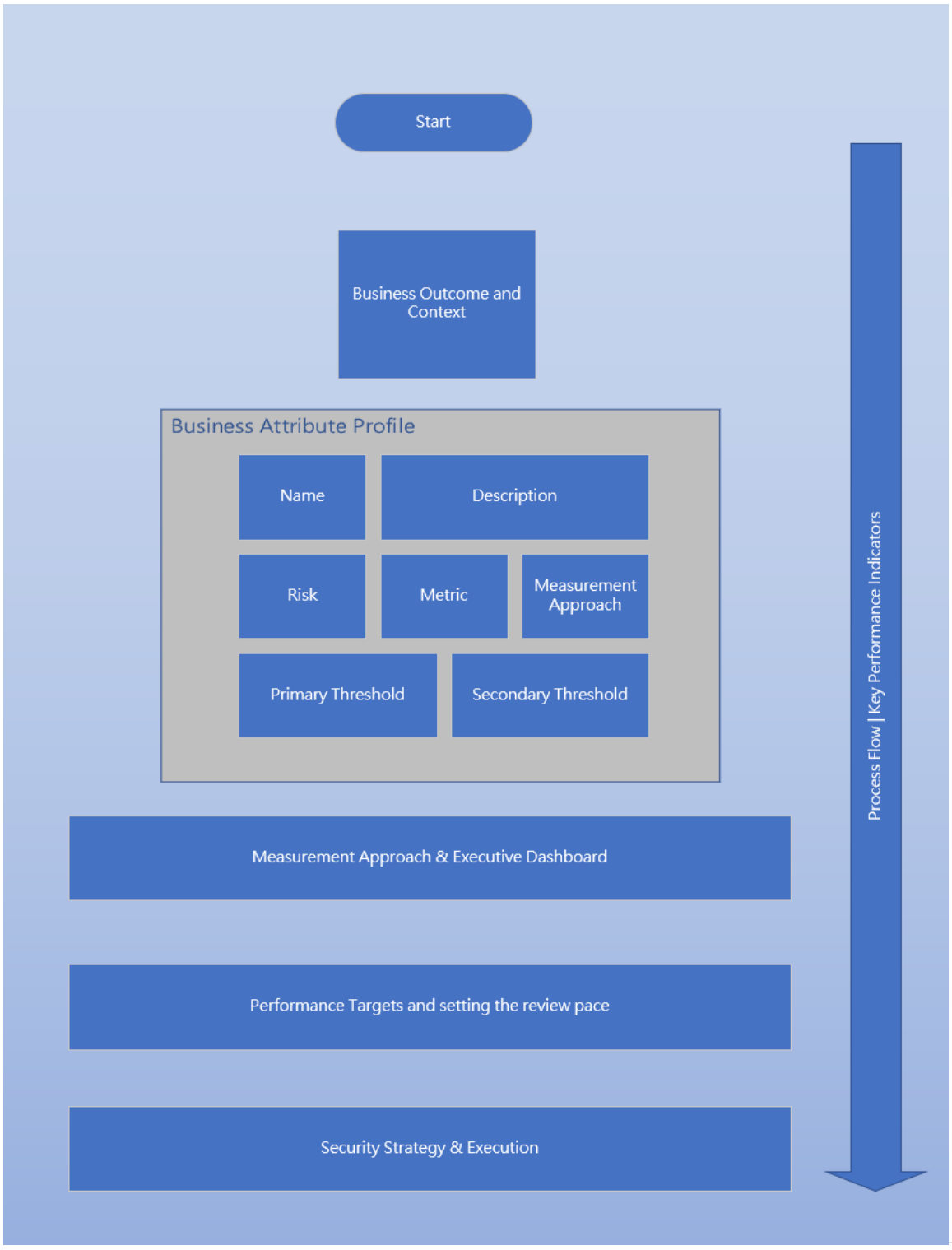
In terms of defining the process flow to identify business attributes is setting a:

- business outcome and context
- name and description for business attribute
- risk, metric and measurement approach
- primary threshold
- secondary threshold

From the monitoring and execution perspective as part of the diagram, we will have:

- measurement approach and executive the dashboard
- Performance and setting the review of the metrics
- lead strategy execution

From the overall business standpoint, it would be possible to set metrics across every phase of this diagram.


Start
Business Outcome and Context
Business Attribute Profile
Name
Description
Risk
Metric
Measurement Approach
Primary Threshold
Secondary Threshold
Measurement Approach & Executive Dashboard
Performance Targets and setting the review pace
Security Strategy & Execution
Process Flow | Key Performance Indicators

**Conceptual Layer**

| Business Attribute | Assets (What) | Motivation (Why) | Process (How) | People (Who) | Location (Where) | Time (When) |
|---|---|---|---|---|---|---|
| Trustworthy | Network Operators and system administrators have limited privileged access to network devices to facilitate troubleshooting activities | High privilege accounts can lead to a full compromise of the environment | Implementation of RBAC or similar approach across all assets | All people with data access | All facilities | 30 days |
| Trustworthy Compliance Confidentiality | Ensure CIA triad is applied | Third-party independent auditors | A different vendor can bring a raw view of the environment. Implementation of a management vendor program for vulnerability assessment | All people with data access | All Data Centers | 15 days |
| Trustworthy | All assets are up to date | Lack of updates can lead to a compromise of the environment | Implementation of patch management systems and dashboard of all assets for compliance | Systems Administrators | All Assets | 7 days |
| Trustworthy | People with Skills and Cybersecurity | Lack of training and education on cybersecurity can lead administrators to be compromised | Training plan and background of security personnel | All personnel | All Facilities | 60 days |

## 2.4 Intended Audience

This cybersecurity architecture is intended for:

- Intergalactic Banking and Financial Services Executives. – The office of Risk Management is responsible for ensuring adequate protection of systems and data within their organizations, and, also identifying and applying the necessary resources to do so. The Office of the CISO (OCISO) focuses on leadership and support of a comprehensive program that provides a proactive approach to mitigating the security threat to the organization, enables the continuous monitoring of the cyber security posture, and supports a wide range of cyber security services supporting implementation of the program. Therefore, the OCISO sets priorities and requirements through high-level policy and guidance, while the ORM is responsible for detailed policy and guidance and implementation in the organization. The office of Risk Management tailors the OCISO-provided guidance and baselines to their mission.
- Cyber Security Personnel - Focuses on Office of Cyber Security staff, but also includes all personnel responsible for managing the Department-wide cyber security programs that provides assistance and guidance in cyber security areas across the organization.
- Network Managers - Network Managers have read access to network management reports, and do not have access to network devices.
- Network Operators - Network Operators have limited privileged access to network devices to facilitate troubleshooting activities.
- System Administrators - System Administrators have full privileged access to network devices.
- Independent Auditors - Audit entities of the organization would be responsible for conducting security audits or assessments on the infrastructure.

## 2.5 Security Standards

This section summarizes the main standards-making bodies that operate in information security and provides an overview of the focus of each body. Are there any security standards which the organization must abide? If so, identify which ones they are and what impact they have on the organization. For this assignment, the main focus framework will be based on SABSA Framework.

- International Organization for Standards (ISO)
- International Electrotechnical Commission (IEC)
- Internet Engineering Task Force (IETF)
- Common Criteria
- American National Standards Institute (ANSI)
- British Standards Institute (BSI)
- International Telecommunication Union (ITU)
- Institute of Electrical and Electronics Engineers (IEEE)
- Information Systems Audit and Control Association (ISACA)
- Object Management Group (OMG)
- Organization for Advancement of Structured Information (OASIS)
- The World Wide Web Consortium (W3C)
- Organization for Economic Co-operation and Development (OECD)
- US Federal Government
- Standards Australia (SAA) and Standards New Zealand (SNZ)
- Japanese Industrial Standards Committee (JISC)
- European Computer Manufacturers Association (ECMA)
- European Telecommunications Standards Institute (ETSI)
- European Forum for Electronic Business (EEMA)
- Wi-Fi Alliance
- Trusted Computing Group (TCG)
- International Security Forum (ISF)
- Vendor Standards
- Internal Security Standards

# 3 Prevention

For each of the following areas which map to the organization's updated cybersecurity strategy, the cybersecurity architecture should be updated.

The architecture for these various areas would address: (these bullets are also addressed in much more detail within the reference Appendix 9)

- Logical - The logical security architecture develops more detail to identify the skeleton of the conceptual framework that was developed during the cybersecurity strategy. The logical layer is largely concerned with the functional view of security, defining a comprehensive set of functional requirements. At this stage, it does not involve the security mechanisms that will be used to deliver those functions.
- Physical - The physical cybersecurity architecture focuses on the physical data structures that are used to realize logical information structures and the physical security mechanisms that implement the logical security services.
- Component - This section looks at the specialized tools and product components of the cybersecurity architecture stopping short of discussing any specific brand or vendor, but covering:
    - How standards are needed to achieve consistency and inter-operability between security architecture components;
    - The role of ASN.1 and XML as fundamental syntax standards on which many other standards are built;
    - The major international, national and industry sector standards-making bodies and their main contributions in providing security-related standards;
    - The most commonly used components in terms of security products and tools, together with a brief overview of their main functional features;
    - Functional security standards based upon XML, including web services comprising various modular building blocks and protocols;
    - The positioning of security protocols within the hierarchical protocol stack.
- Operational – Although this will be addressed by the organization, it should still be noted that this area is important and needed for a complete cybersecurity architecture. At this stage, this document would only address the framework for the operational processes. The organization's security architects therefore need to involve their operations colleagues in the work, so that what is designed will be workable. It will be up

to those operational teams to define the detailed procedures and so on, but at this stage, a framework should identify which processes, procedures and activities are needed and how they relate to one another.

Cybersecurity architecture around the area of prevention would address items, such as the following sub-sections below.

## 3.1 Entity Security Services

Entity security addresses areas such as:

- Entity unique naming
    - Naming standards
    - Naming procedure
    - Directory system
- Entity registration
    - Registration policy
    - Registration authority system
    - Registration procedure
- Entity public key certification
    - Certification policy
    - Certification authority system
    - Certification procedure
    - Certificate syntax standards
    - Certificate publishing mechanism (directory)
    - Certificate revocation list (CRL)
    - CRL publishing and management (directory)
- Entity credentials certification
    - Certification policy
    - Certification authority system
    - Certification procedure
    - Certificate syntax standards

    - Certificate publishing mechanism (directory)
    - Certificate revocation list (CRL)
    - CRL publishing and management (directory)
- Directory service
    - Directory system
    - Directory access protocols
    - Directory object and attribute syntax rules
    - Directory replication
- Entity authorization
    - Roles
    - Fixed role associations with entities
    - Real-time role association with entities
    - Authorization certificates
- Entity authentication
    - Login procedure
    - User passwords and tokens
    - Client user agents for authentication
    - Authentication exchange protocols
    - Authentication server system
    - Directory system
- User authentication
- Device authentication

## 3.2 Communications Security Services

Communications security addresses areas such as:

- Session authentication
    - Mutual two-way and three-way authentication exchanges
    - Session context (finite state machine)
- Message origin authentication
    - Message source identifiers protected by:
        - Message integrity checksums
        - Digital signatures
        - Hashing
- Message integrity protection
    - Message integrity checksums
    - Digital signatures
    - Hashing
- Message content confidentiality
    - Message contents encryption
    - Encryption key management
    - Routing control to physically secure networks
- Security measurement and metrics
- Security administration (privilege management)
- User support
    - Help desk
    - Trouble ticketing system
- Physical security services
- Environmental security services
- Non-repudiation
    - Digital signatures
    - Notarization servers

    - Transaction logs
    - Trusted third party certification and arbitration
- Message replay protection
- Traffic flow confidentiality
    - Traffic padding

## 3.3 Application and System Security

Application and system security addresses areas such as:

- Entity authorization
    - Roles
    - Fixed role associations with entities
    - Real-time role association with entities
    - Authorization certificates
- Logical access control
    - Local access control agents
    - Local role access control lists (ACLs)
    - Central access manager (CAM)
    - CAM role ACLs
    - Central application access control agents
    - Central application role ACLs
    - Database management system mechanisms
    - File system mechanisms
- Audit trails
    - Event logs
    - Event log integrity protection mechanisms
    - Event log browsing tools
    - Event log analysis tools

    - Reporting tools
- Stored data integrity protection
- Stored data confidentiality
    - Logical access control mechanisms
    - Physical access control mechanisms
    - Stored data encryption
    - Media storage security
    - Media disposal procedures
- Software data integrity protection
    - Logical access control mechanisms
    - Physical access control mechanisms
    - Stored data encryption
    - Media storage security
    - Media disposal procedures
- Software licensing management
    - Software metering
- System configuration protection
    - Production system configuration control
    - Production system change control
    - Production system management authorization
    - Cryptographic checksums on configuration data files
    - Regular inspection of configuration data files and checksums
- Data replication and backup
    - Regular backup copying
    - Backup media management: labelling, indexing, transport, storage, retrieval, media recycling, media disposal
- Software replication and backup
    - Master software media management: labelling, indexing, transport, storage, retrieval

- Trusted time
    - Secure time server with clock
    - Secure time server protocols
- User interface for security
    - GUI login screens
    - GUI security message screens
    - Single sign-on mechanism
    - Ergonomic design of authentication devices
    - Help desk for security problem resolution

## 3.4 Security Management

Security management addresses areas such as:

- Security policy management
    - Data content monitoring and filtering
    - Real-time system monitoring
- Security service management
    - Security service management sub-system
    - Secure management protocols
    - Management agents in managed components
    - Access control at all agents and sub-systems security alarms
- Security training and awareness
    - Training courses
    - Training manuals and documentation
    - Publicity campaigns
- Security operations management
    - Operator authentication mechanisms
    - Operator activity logs
    - Operations event logs

- Security provisioning
    - Security service management sub-system
    - Secure management protocols
    - Management agents in managed components
    - Access control at all agents and sub-systems security alarms
- Security monitoring
    - User activity logs
    - Application event logs
    - Operator activity logs
    - Management event logs
    - Event log browsing and analysis
- Security measurement and metrics
    - Cryptographic test mechanisms
    - Inspection tools
    - Penetration testing
    - Statistical tests
- Security administration (privilege management)
    - Security service management sub-system
    - Secure management protocols
    - Management agents in managed components
    - Access control at all agents and sub-systems security alarms
- User Support
    - Help desk
    - Trouble ticketing system
- Personnel Security
    - Hiring, background checking and vetting procedures
    - Training courses, booklets, publicity campaigns
    - Disciplinary procedures

- Physical Security Devices
- Environmental security services
    - Site-selection procedures
    - Fire prevention, detection and quenching
    - Flood avoidance, detection and removal
    - Air temperature and humidity controls
    - Electrical power protection mechanisms

# 4 Containment

For each of the following areas which map to the organization's updated cybersecurity strategy, the cybersecurity architecture should be updated. The architecture for these various areas would address: (these bullets are also addressed in much more detail within the reference Appendix 9)

- Logical - The logical security architecture develops more detail to identify the skeleton of the conceptual framework that was developed during the cybersecurity strategy. The logical layer is largely concerned with the functional view of security, defining a comprehensive set of functional requirements. At this stage, it does not involve the security mechanisms that will be used to deliver those functions.
- Physical - The physical cybersecurity architecture focuses on the physical data structures that are used to realize logical information structures and the physical security mechanisms that implement the logical security services.
- Component - This section looks at the specialized tools and product components of the cybersecurity architecture stopping short of discussing any specific brand or vendor, but covering:
    - How standards are needed to achieve consistency and inter-operability between security architecture components;
    - The role of ASN.1 and XML as fundamental syntax standards on which many other standards are built;
    - The major international, national and industry sector standards-making bodies and their main contributions in providing security-related standards;
    - The most commonly used components in terms of security products and tools, together with a brief overview of their main functional features;
    - Functional security standards based upon XML, including web services comprising various modular building blocks and protocols;
    - The positioning of security protocols within the hierarchical protocol stack.
- Operational – Although this will be addressed by the organization, it should still be noted that this area is important and needed for a complete cybersecurity architecture. At this stage, this document would only address the framework for the operational processes. The organization's security architects therefore need to involve their operations colleagues in the work, so that what is designed will be workable. It will be up to those operational teams to define the detailed procedures and so on, but at this

stage, a framework should identify which processes, procedures and activities are needed and how they relate to one another.

Containment addresses areas such as:

- Entity authorization
- Stored data confidentiality
    - Logical access control mechanisms
    - Physical access control mechanisms
    - Stored data encryption
    - Media storage security
    - Media disposal procedures
- Software integrity protection
    - Development lifecycle controls
    - Delivery and installation controls
    - Production system configuration control
    - Production system change control
    - Production system management authorization
    - Crypto checksums on object code images
    - Regular inspection of object code images and checksums
    - Anti-virus tools
- Physical security
    - Secure premises with locks and guards
    - Locked rooms for servers, operations and communications
    - Physical protection for cabling
    - Authorization procedures
    - Identification badges and visitor procedures
    - Supervision of contract engineers
- Environmental security
- Security training and awareness

# 5 Detection and Notification

For each of the following areas which map to the organization's updated cybersecurity strategy, the cybersecurity architecture should be updated. The architecture for these various areas would address: (these bullets are also addressed in much more detail within the reference Appendix 9)

- Logical - The logical security architecture develops more detail to identify the skeleton of the conceptual framework that was developed during the cybersecurity strategy. The logical layer is largely concerned with the functional view of security, defining a comprehensive set of functional requirements. At this stage, it does not involve the security mechanisms that will be used to deliver those functions.
- Physical - The physical cybersecurity architecture focuses on the physical data structures that are used to realize logical information structures and the physical security mechanisms that implement the logical security services.
- Component - This section looks at the specialized tools and product components of the cybersecurity architecture stopping short of discussing any specific brand or vendor, but covering:
    - How standards are needed to achieve consistency and inter-operability between security architecture components;
    - The role of ASN.1 and XML as fundamental syntax standards on which many other standards are built;
    - The major international, national and industry sector standards-making bodies and their main contributions in providing security-related standards;
    - The most commonly used components in terms of security products and tools, together with a brief overview of their main functional features;
    - Functional security standards based upon XML, including web services comprising various modular building blocks and protocols;
    - The positioning of security protocols within the hierarchical protocol stack.
- Operational – Although this will be addressed by the organization, it should still be noted that this area is important and needed for a complete cybersecurity architecture. At this stage, this document would only address the framework for the operational processes. The organization's security architects therefore need to involve their operations colleagues in the work, so that what is designed will be workable. It will be up to those operational teams to define the detailed procedures and so on, but at this

stage, a framework should identify which processes, procedures and activities are needed and how they relate to one another.

Detection and notification addresses areas such:

- Message integrity protection
- Stored data integrity protection
    - Message integrity checksums
    - Digital signatures
    - Hashing
- Security monitoring
- Intrusion detection
    - Intrusion signature analysis on network traffic
    - Real-time system monitoring
    - Alarms
- Security alarm management
    - Security alarms
    - Security alarm monitoring
- Security training and awareness
- Security measurement and metrics

# 6 Event Collection and Event Tracking

For each of the following areas which map to the organization's updated cybersecurity strategy, the cybersecurity architecture should be updated. The architecture for these various areas would address: (these bullets are also addressed in much more detail within the reference Appendix 9)

- Logical - The logical security architecture develops more detail to identify the skeleton of the conceptual framework that was developed during the cybersecurity strategy. The logical layer is largely concerned with the functional view of security, defining a comprehensive set of functional requirements. At this stage, it does not involve the security mechanisms that will be used to deliver those functions.
- Physical - The physical cybersecurity architecture focuses on the physical data structures that are used to realize logical information structures and the physical security mechanisms that implement the logical security services.
- Component - This section looks at the specialized tools and product components of the cybersecurity architecture stopping short of discussing any specific brand or vendor, but covering:
    - How standards are needed to achieve consistency and inter-operability between security architecture components;
    - The role of ASN.1 and XML as fundamental syntax standards on which many other standards are built;
    - The major international, national and industry sector standards-making bodies and their main contributions in providing security-related standards;
    - The most commonly used components in terms of security products and tools, together with a brief overview of their main functional features;
    - Functional security standards based upon XML, including web services comprising various modular building blocks and protocols;
    - The positioning of security protocols within the hierarchical protocol stack.
- Operational – Although this will be addressed by the organization, it should still be noted that this area is important and needed for a complete cybersecurity architecture. At this stage, this document would only address the framework for the operational processes. The organization's security architects therefore need to involve their operations colleagues in the work, so that what is designed will be workable. It will be up to those operational teams to define the detailed procedures and so on, but at this

stage, a framework should identify which processes, procedures and activities are needed and how they relate to one another.

Event collection and event tracking addresses areas such:

- Audit trails
- Security operations management
- Security monitoring
- Security measurement and metrics

# 7 Recovery and Restoration

For each of the following areas which map to the organization's updated cybersecurity strategy, the cybersecurity architecture should be updated. The architecture for these various areas would address: (these bullets are also addressed in much more detail within the reference Appendix 9)

- Logical - The logical security architecture develops more detail to identify the skeleton of the conceptual framework that was developed during the cybersecurity strategy. The logical layer is largely concerned with the functional view of security, defining a comprehensive set of functional requirements. At this stage, it does not involve the security mechanisms that will be used to deliver those functions.
- Physical - The physical cybersecurity architecture focuses on the physical data structures that are used to realize logical information structures and the physical security mechanisms that implement the logical security services.
- Component - This section looks at the specialized tools and product components of the cybersecurity architecture stopping short of discussing any specific brand or vendor, but covering:
    - How standards are needed to achieve consistency and inter-operability between security architecture components;
    - The role of ASN.1 and XML as fundamental syntax standards on which many other standards are built;
    - The major international, national and industry sector standards-making bodies and their main contributions in providing security-related standards;
    - The most commonly used components in terms of security products and tools, together with a brief overview of their main functional features;
    - Functional security standards based upon XML, including web services comprising various modular building blocks and protocols;
    - The positioning of security protocols within the hierarchical protocol stack.
- Operational – Although this will be addressed by the organization, it should still be noted that this area is important and needed for a complete cybersecurity architecture. At this stage, this document would only address the framework for the operational processes. The organization's security architects therefore need to involve their operations colleagues in the work, so that what is designed will be workable. It will be up to those operational teams to define the detailed procedures and so on, but at this

stage, a framework should identify which processes, procedures and activities are needed and how they relate to one another.

Recovery and restoration addresses areas such:

- Incident response
    - Data collection and analysis
    - Incident assessment procedures
    - Response action management procedures
- Data replication and backup
- Software replication and backup
- Disaster recovery
    - Data backups
    - Software backups
    - Data restoration procedures
    - Off-site backup storage
    - Backup media management: indexing, labelling, transport, storage, retrieval, recycling, disposal
    - Redundancy of hardware
    - Redundancy of communications lines
    - Recovery plans
    - Recovery procedures
- Crisis management
    - Vested authority in a crisis manager and crisis management team
    - Assessment procedures
    - Escalation procedures
    - Activation procedures

# 8 Assurance

For each of the following areas which map to the organization's updated cybersecurity strategy, the cybersecurity architecture should be updated. The architecture for these various areas would address: (these bullets are also addressed in much more detail within the reference Appendix 9)

- Logical - The logical security architecture develops more detail to identify the skeleton of the conceptual framework that was developed during the cybersecurity strategy. The logical layer is largely concerned with the functional view of security, defining a comprehensive set of functional requirements. At this stage, it does not involve the security mechanisms that will be used to deliver those functions.
- Physical - The physical cybersecurity architecture focuses on the physical data structures that are used to realize logical information structures and the physical security mechanisms that implement the logical security services.
- Component - This section looks at the specialized tools and product components of the cybersecurity architecture stopping short of discussing any specific brand or vendor, but covering:
    - How standards are needed to achieve consistency and inter-operability between security architecture components;
    - The role of ASN.1 and XML as fundamental syntax standards on which many other standards are built;
    - The major international, national and industry sector standards-making bodies and their main contributions in providing security-related standards;
    - The most commonly used components in terms of security products and tools, together with a brief overview of their main functional features;
    - Functional security standards based upon XML, including web services comprising various modular building blocks and protocols;
    - The positioning of security protocols within the hierarchical protocol stack.
- Operational – Although this will be addressed by the organization, it should still be noted that this area is important and needed for a complete cybersecurity architecture. At this stage, this document would only address the framework for the operational processes. The organization's security architects therefore need to involve their operations colleagues in the work, so that what is designed will be workable. It will be up to those operational teams to define the detailed procedures and so on, but at this

stage, a framework should identify which processes, procedures and activities are needed and how they relate to one another.

Assurance addresses areas such:

- Audit trails
- Security audit
    - Independent inspection
    - Regular scanning with system audit tools
- Security monitoring
- Security measurement and metrics

# 9 Appendices

## 9.1 A Model for Security Architecture Development

The figure shown below is an example of a cybersecurity architecture model from SABSA.

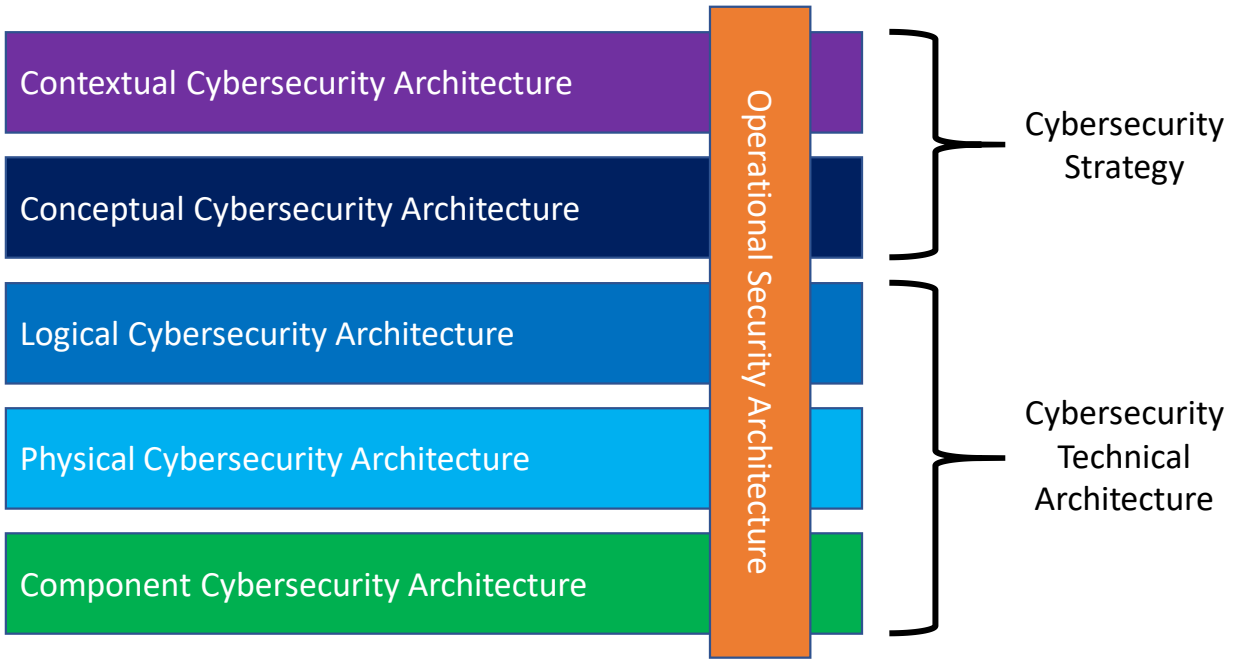



Figure 1 – Security Architecture Development

The contextual cybersecurity architecture is a description of the business context in which an organization's systems must be securely designed, built, and operated. The contextual cybersecurity architecture is concerned with:

- What? The business, its assets to be protected (brand, reputation, etc.) and the business needs for information security (security as a business enabler, secure electronic business, operational continuity and stability, compliance with the law, etc.).
- Why? The business risks expressed in terms of assets, goals, success factors and the threats, impacts and vulnerabilities that put these at risk, driving the need for business security (brand protection, fraud prevention, loss prevention, legal obligations, business continuity, etc.).
- How? The business processes that require security (business interactions and transactions, business communications, etc.).
- Who? The organizational aspects of business security (management structures, supply chain structures, out-sourcing relationships, strategic partnerships).

- Where? The business geography and location-related aspects of business security (the global village marketplace, distributed corporate sites, remote working, etc.).
- When? The business time dependencies and time-related aspects of business security in terms of both performance and sequence (business transaction throughput, lifetimes and deadlines, just-in-time operations, time-to-market, etc.).

The conceptual cybersecurity architecture defines the principles and fundamental concepts that guide the selection and organization of the logical and physical elements at the lower layers. The conceptual cybersecurity architecture is concerned with:

- What? Capturing business requirements.
- Why? Control objectives are derived directory from an analysis of business operational risks and are a conceptualization of business motivation for security.
- How? For every major area of the business requirements identified in the contextual security architecture, there will be a security strategy or group of strategies that supports it. These security strategies and layering principles include areas such as application security, network security, cryptographic strategy, role-based access strategy.
- Who? The security entities and their trust relationships. This involved identifying who is involved in security management, in terms of entity relationship models, and the trust framework within which entities interact with one another.
- Where? The security domain model. This defines where you want to achieve the protection conceptualized in terms of security domains, both logical and physical.
- When? The time dependence on security. This identifies lifetimes and expiration deadlines, timestamping, time-sensitive business transactions, and performance criteria.

The logical cybersecurity architecture involves the identification and specification of the logical architectural elements of an overall system. This view models the business as a system, with system components that are themselves sub-systems. It shows the major architectural security elements in terms of logical security services and describes the logical flow of control and the relationships between these logical elements. The logical cybersecurity architecture is concerned with:

- What? Business information is a logical representation of the real business. It is this business information that needs to be secured.
- Why? Specifying the security policy requirements (high-level security policy, registration authority policy, certification authority policy, physical domain policies, logical domain policies, etc.) for securing business information.

- How? Specifying the logical security services (entity authentication, confidentiality protection, integrity protection, non-repudiation, system assurance, etc.) and how they fit together as common re-usable building blocks into a complex security system that meets the overall business requirements.
- Who? Specifying the entities (users, security administrators, auditors, etc.) and their inter-relationships, attributes, authorized roles and privilege profiles in the form of a schema.
- Where? Specifying the security domains and inter-domain relationships (logical security domains, physical security domains, security associations).
- When? Specifying the security processing cycle (registration, certification, login, session management, etc.).

The physical cybersecurity architecture produces a set of logical abstractions that describe the system to be built. These describe the actual technology model and specifies the functional requirements of the various system components. The logical security services are now expressed in terms of the physical security mechanisms and machines that will be used to deliver these services. The physical cybersecurity architecture is concerned with:

- What? Specifying the business data model and the security-related data structures (tables, messages, pointers, certificates, signatures, etc.).
- Why? Specifying rules that drive logical decision-making within the system (conditions, practices, procedures and actions).
- How? Specifying security mechanisms (encryption, access control, digital signatures, virus scanning, etc.) and the physical machines upon which these mechanisms will be hosted.
- Who? Specifying the people dependency in the form of the users, the applications that they use and the security user interface (screen formats and user interactions).
- Where? Specifying security technology infrastructure (physical layout of the hardware, software and communications lines).
- When? Specifying the time dependency in the form of execution control structures (sequences, events, lifetimes and time intervals).

The component cybersecurity architecture specifies products and system components.

These include hardware-related, software-related, and service-oriented components and standards. The component cybersecurity architecture is concerned with:

- What? Data field specifications, address specifications and other detailed data structure specifications.
- Why? Security standards.

- How? Products and tools (both hardware and software).
- Who? User identities, privileges, functions, actions and ACLs.
- Where? Computer processes, node addresses, and inter-process protocols.
- When? Security step timings and sequencing.

The operational cybersecurity architecture is concerned with classical systems operations work. The focus of attention is only on the security-related parts of that work, such as defining:

- What? The security of operational business data and information is maintained.
- Why? Manage operational risks to minimize operational failures and disruptions.
- How? Performing specialized security-related operations (user security administration, system security administration, data back-ups, security monitoring, emergency response procedures, etc.).
- Who? Providing operational support for the security-related needs of all users and their applications (business users, operators, administrators, etc.).
- Where? Maintaining the system integrity and security of all operational platforms and networks (by applying operational security standards and auditing the configuration against these standards).
- When? Scheduling and executing a timetable of security-related operations.

### 9.1.1 Contextual Security Architecture

Contextual security architecture is describing the business needs for information security. The value of information security is related to the business value protected. Information security has no intrinsic value of its own. Its only possible value is that it protects something that has explicit value to the business. Therefore, you must begin the process of defining your enterprise-wide information security architecture by first identifying the things that you consider to be valuable that are affected by information security. Once those are defined, risk modeling should be performed.

The most commonly accepted model for risk involves some basic concepts:

- Assets – things that are of value to your business that you want to protect;
- Threats – potential damaging events that put your assets in danger;
- Vulnerabilities – weaknesses in your operational business procedures or systems that will allow a threat to materialize and exploit an asset, causing an impact.
- Impacts – the potential outcome of a threat materializing and causing damage to your assets;

Once basic risk modeling is performed, identified risks need to be mitigated. Risk mitigation is the process of setting control objectives and implementing controls through the security architecture.

Once control objectives are identified, then they can begin driving conceptual security architecture.

**Note**: This is expected to have been completed during the Cybersecurity Strategy work.

### 9.1.2 Conceptual Security Architecture

Now that control objectives have been identified, the conceptual security architecture can begin. Control objectives will drive the following work:

You will need to decide which of these initiatives and services you require in your cybersecurity strategy to meet the requirements and policies that you have derived.

| Defensive Initiative | Security Services | |
|---|---|---|
| **Prevention** | Entity Security Services | Entity unique naming |
| | | Entity registration |
| | | Entity public key certification |
| | | Entity credentials certification |
| | | Directory service |
| | | Entity authorization |
| | | Entity authentication |
| | | User authentication |
| | | Device authentication |
| | Communications Security Services | Session authentication |
| | | Message origin authentication |
| | | Message integrity protection |
| | | Message content confidentiality |
| | | Security measurement and metrics |
| | | Security administration (privilege management) |
| | | User support |
| | | Physical security services |
| | | Environmental security services |
| | | Non-repudiation |
| | | Message replay protection |
| | | Traffic flow confidentiality |
| | Application and System Security Services | Entity authorization |
| | | Logical access control |
| | | Audit trails |
| | | Stored data integrity protection |
| | | Stored data confidentiality |
| | | Software integrity protection |
| | | Software licensing management |
| | | System configuration protection |
| | | Data replication and backup |
| | | Software replication and backup |
| | | Trusted time |
| | | User interface for security |
| | Security Management Services | Security policy management |
| | | Security training and awareness |
| | | Security operations management |

| Defensive Initiative | Security Services | |
|---|---|---|
| | | Security provisioning |
| | | Security monitoring |
| | | Security measurement and metrics |
| | | Security administration (privilege management) |
| | | User Support |
| | | Physical Security Devices |
| | | Environmental security services |
| **Containment** | Entity authorization | |
| | Stored data confidentiality | |
| | Software integrity protection | |
| | Physical security | |
| | Environmental security | |
| | Security training and awareness | |
| **Detection and Notification** | Message integrity protection | |
| | Stored data integrity protection | |
| | Security monitoring | |
| | Intrusion detection | |
| | Security alarm management | |
| | Security training and awareness | |
| | Security measurement and metrics | |
| **Event Collection and Event Tracking** | Audit trails | |
| | Security operations management | |
| | Security monitoring | |
| | Security measurement and metrics | |
| **Recovery and Restoration** | Incident response | |
| | Data replication and backup | |
| | Software replication and backup | |
| | Disaster recovery | |
| | Crisis management | |
| **Assurance** | Audit trails | |
| | Security audit | |
| | Security monitoring | |
| | Security measurement and metrics | |

## 9.2 Logical Cybersecurity

The logical security architecture develops more detail to identify the skeleton of the conceptual framework that was developed during the cybersecurity strategy. The logical layer is largely concerned with the functional view of security, defining a comprehensive set of functional requirements. At this stage, it does not involve the security mechanisms that will be used to deliver those functions. Those are part of the next later; the physical security architecture.

### 9.2.1 Security Policy Architecture

Security policy architecture – a hierarchical model of policy documentation and how it fits together. As seen in the figure below, Security policy exists at several different levels.

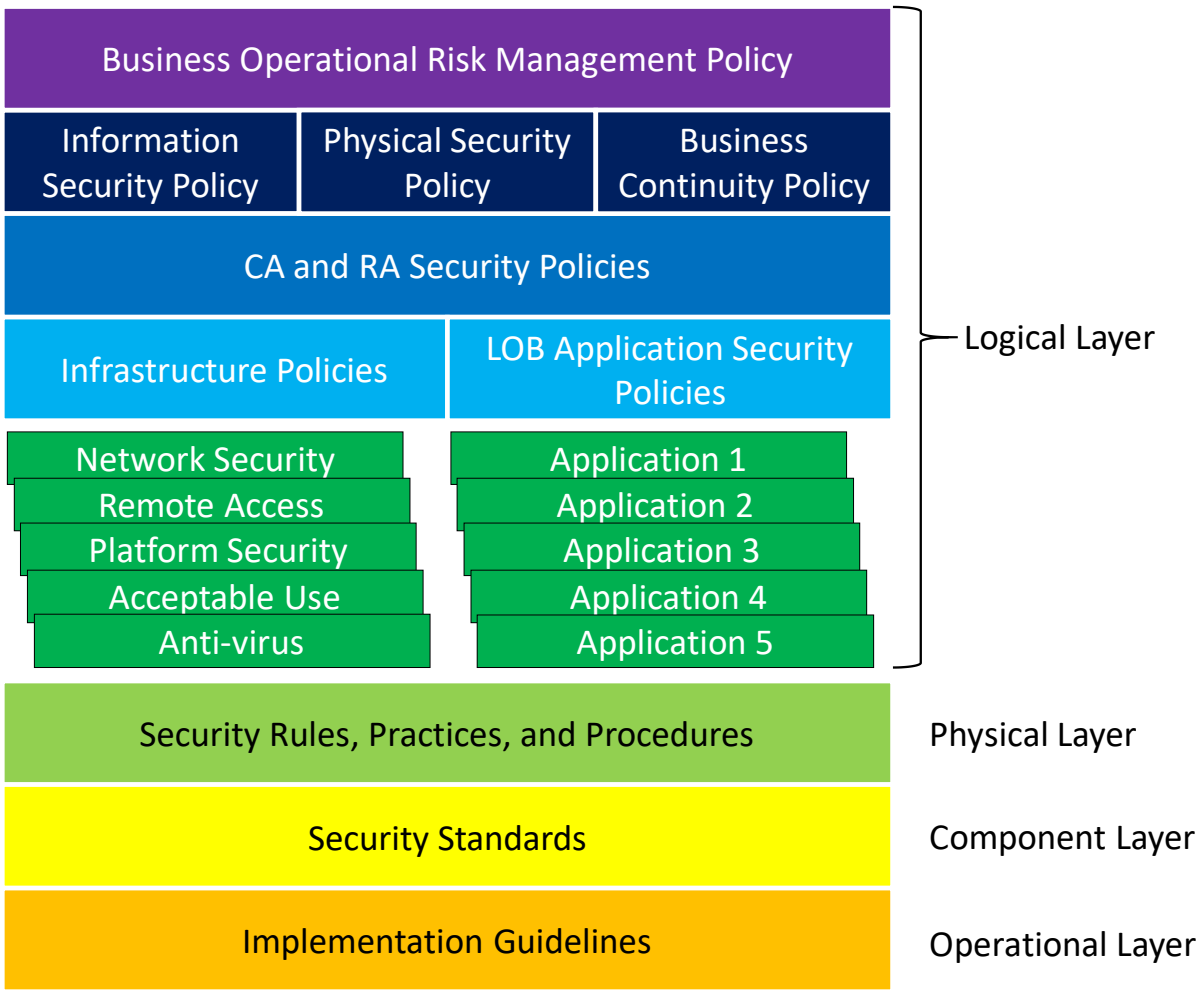



Figure 2 – Hierarchical Policy Architecture

### 9.2.2 Individual Security Policies

The individual security policies, or at least templates and guidelines for their production.

Security policies are statements of what type of security and how much should be applied to protect the business in various ways. Security policy is positioned at the logical layer of the security architecture model and is derived directly from several drivers in the cybersecurity strategy. The control objectives are strong drivers of security policy.

A security policy defines what is meant by security within a security domain, the high-level rules for achieving this security and the activities that are to be authorized to achieve security objectives. The policy also defines how entities outside the domain can interact with entities inside the domain.

### 9.2.3 Entity Schema

The entity schema to be applied in the enterprise-wide (logical) directory, with associated models for privilege profiles, authorizations, authentication attributes, etc. This section would cover such topics as:

- Entity Schemas
- Role Associations
- Authorization, Privilege Profiles, and Credentials
- Certificates and Tickets

### 9.2.4 Specific Security Domains

The specific security domains with a description of their logical make-up, their individual security policies and the security associations that exist both intra-domain and inter-domain. These would cover:

- Network Domains
- Middleware Domains
- Application Domains
- Security Service Management Domains
- Policy Interactions between Domains

### 9.2.5 Logical Security Processing Cycle

A description of the logical security processing cycle. This involves certain security management activities, such as:

- Introducing and registering new organizational entities;
- Introducing and registering new users;
- Setting up authorized privileges;
- Registration renewal;
- Certificate issue and renewal;
- Provisioning and configuring equipment throughout the environment.

### 9.2.6 Improvements program

An improvements program to gain short-term advantages and to deliver early wins from the security architecture program. This is comprised of short-term projects to achieve quick wins.

## 9.3 Physical Cybersecurity

The physical cybersecurity architecture focuses on the physical data structures that are used to realize logical information structures and the physical security mechanisms that implement the logical security services.

### 9.3.1 Updated Business Data Model

The security architecture team will not develop the business data model itself, but will be updated with relevant security data, such as passwords, usernames, certificates, etc. This covers areas such as:

- File and Directory access control,
- File encryption,
- Database security,
- Security mechanisms in SQL databases,
- Distributed databases, and
- Data storage.

### 9.3.2 Security rules, practices, and procedures

Rules are an interpretation of policies. This section defines security rules, practices and procedures that will be required. At this stage, the details of the procedures and practices will not be written. The statement will describe only certain procedures and practices that will be needed to implement the policies defined at the logical layer. Templates for creating these procedures and practices may also be defined here. This would include such items as:

- Security rules
- Security practices and procedures

### 9.3.3 Applications and user communities

A list of applications and user communities, with a security user interface design for each type. In the future, as more applications are added, this may need to be updated. As with the security mechanisms, the number of user interface types should be minimized to avoid complexity and to provide generic, re-usable, modular approaches to the construction of new applications. A user interface module with a defined API would be a good architectural approach.

This section describes the security mechanisms that are commonly applied to implement user security and application security. Among these mechanisms is the user password, which is an important element of the security user interface, and there is some discussion of the issues that surround the use of this mechanism.

The security mechanisms by which these services are implemented are fairly straightforward. They include:

- Directory Mechanisms
- Central Access Manager Mechanisms
- Database Mechanisms
- File System Mechanisms
- Operating System Mechanisms
- Application Mechanisms
- User Authentication Mechanisms
- Password Management

### 9.3.4 Physical Layout

The physical layout of the platforms and networks, probably in diagrammatic form. This is a physical representation, defining the number of physical computer boxes, physical communications lines and physical networking equipment items – how many, what type and where.

### 9.3.5 Capacity Planning

A statement of capacity planning. Given the throughput of the devices, the processing power of computers and the bandwidth of communications lines, how many of each will be required to handle the expected load? This section addresses items such as:

- Platform security
- Hardware security
- Network Topology
- Directory Topology

### 9.3.6 Resilience Model

A description of the resilience model provided by redundancy of boxes and connections. The resilience model is integral to the physical layout model, providing redundant capacity in resilient configurations.

### 9.3.7 Control Structure Execution model

The control structure execution model needed to execute the logical security processing cycle from the layer above.

## 9.4 Component Cybersecurity

This section looks at the specialized tools and product components of the cybersecurity architecture stopping short of discussing any specific brand or vendor, but covering:

- How standards are needed to achieve consistency and inter-operability between security architecture components;
- The role of ASN.1 and XML as fundamental syntax standards on which many other standards are built;

- The major international, national and industry sector standards-making bodies and their main contributions in providing security-related standards;
- The most commonly used components in terms of security products and tools, together with a brief overview of their main functional features;
- Functional security standards based upon XML, including web services comprising various modular building blocks and protocols;
- The positioning of security protocols within the hierarchical protocol stack.

### 9.4.1 Detailed Security Data Structures

This section discusses the basic syntax standards that are used to create standardized data structures for the security-related protocols that are used to exchange this data regarding:

- Inter-operability
- Abstract Syntax notation
- Extensible Markup Language
- Relationship between ASN.1 and XML
- Standard Security Data Structures

### 9.4.2 Security Products & Tools

A list with descriptions and specifications of all strategic technologies, products and tools that have been selected, with guidance for project teams as to how, why, where and when they should be used.

This table lists some of the most common types of security tools and products and gives an overview of the most commonly found features of those components.

Table 1 – Security Tools and Products

| Component Type | Common Features / Mechanisms |
|---|---|
| Anti-piracy tools | Preventing the illegal copying and distribution of software |
| Anti-virus scanners | Scanning for known viruses and other malicious software, and repairing any damaged files (although the repair may not be perfect and therefore may not be the correct way to proceed) |
| Anti-theft devices | Preventing the theft of equipment items such as PCs |
| Biometric devices | Providing personal authentication based on measurement of a bodily feature – such as fingerprint, retina pattern, and facial geometry |

| Component Type | Common Features / Mechanisms |
|---|---|
| Boot-protection software | Preventing the booting of a PC from a diskette to get unauthorized access to the hard drive |
| Business continuity planning and disaster recovery planning tools | Supporting the collection and management of planning information |
| CCTV monitoring | Physical site surveillance |
| Computer forensics tools | Recovering deleted data and piecing together a history of activity |
| Content filtering for e-mail | Detecting and filtering out unacceptable content |
| Content filtering for web browsing | Detecting and filtering out unacceptable content |
| Cryptographic hardware | Providing high-performance cryptographic processing, high-security key storage, secure time source, random number generation for key management, tamper-resistant enclosures |
| Cryptographic software tool-kits | Run-time libraries for data encryption, authentication, digital signatures and certificate processing |
| Data backup management systems | Copying and storage management, and restoration to a previous business position |
| Directory products | Providing directory services |
| Document safes | Protecting documents from theft and fire damage |
| E-mail encryption and authentication products | Providing privacy and authentication for e-mail messages |
| Enterprise security management tools | Managing a wide range of security services across multiple platforms |
| Fault-tolerant computing solutions | Resilient computing platforms that will survive failure of components |
| File encryption products | Encrypting files either for transmission or for storage |
| Firewalls | Filtering network traffic according to source, destination and content to allow only authorized traffic |
| Intrusion detection systems | Looking for unauthorized activity from intruders both in the network and on host platforms |
| LAN security products | Providing security functionality in local area networks |
| Operating platforms | Logical access control and integrity protection |
| Personal authentication tokens and devices | Multi-factor authentication of users |
| Physical security alarms | Intruder alarms and fire alarms in buildings and computer suites |
| PKI software | Digital certificate management and the cryptographic services that it supports |
| Risk assessment tools | Software packages to capture and process risk data |

| Component Type | Common Features / Mechanisms |
|---|---|
| Role-based access control solutions | Centralized role-based access control management and authentication of users |
| Secure middleware products | Providing secure node-to-node communications and an API for applications to call security services |
| Security auditing tools | Automated inspection tools to check the configuration of an operating platform or application |
| Security shells | Add-on software products to provide additional levels of access control to standard operating systems |
| Single sign-on authentication service solutions | Centralized authentication servers integrating distributed applications and providing an authentication front end with single sign-on |
| Smart cards | A self-contained computer on a plastic card with its own onboard authentication and access control functions |
| Software license management tools | Managing the distribution of licensed software to ensure compliance with the license |
| Uninterruptible power supplies | Protecting against electrical power failure |
| VPN products | Virtual private networks built using IPSec or SSL |
| Vulnerability scanning tools | Looking for holes in the network or host configurations |
| Wireless security products | Preventing eavesdropping and authenticating nodes |

### 9.4.3 Identifies, Functions, Actions, ACLs

This section discusses the main functional security protocol standards and their application. It is focused around the webservices standards that are currently being used to build the infrastructure for digital business within:

- Web services
- XML Schema
- Simple Object Access Protocol (SOAP)
- Web Services Security and Trust
- XML Encryption
- XML Signature
- SOAP Extensions: Digital Signature
- XML Key Management
- Security service Markup Language (S2ML)
- Security Assertion Markup Language (SAML)
- Web Services Security Language (WS-Security)
- eXtensible Access Control Markup Language (XACML)
- eXtensible Business Reporting Language (XBRL)

- XML Benefits
- XML Security Architecture Issues
- XML Firewalls
- Non-Web Applications

### 9.4.4 Processes, nodes, addresses, and protocols

This section describes some more security-related protocols and describes how these fit into the hierarchical protocol stack, such as:

- Hypertext Transfer Protocol (HTTP)
- Secure HTTP (S-HTTP)
- HTTPS
- SSL and TLS
- IPSec
- DNSSec
- SASL

### 9.4.5 Security step timing and sequencing

The timing and sequencing of security steps is primarily driven by business requirements, such as user expectations, business deadlines, volume throughput requirements, and so on. However, in this section, we must deal with the nuts and bolts of how that timing and sequencing is to be achieved in practice. Much of this will depend upon the performance and efficiency of the various components that you have assembled to build the architecture.

## 9.5 Operational Cybersecurity

### 9.5.1 Framework for assurance of operational continuity

Operational continuity should be taken in its very broadest sense here. This means that you need assurance that the service capabilities are being provided at a level compatible with the performance targets that you have set for each one. There are several types of inspection used to provide assurance:

- Security audits and security reviews of an organizational unit against a suitable code of practice (such as ISO/IEC 177991);
- Security audits and security reviews of a system against a set of pre-determined security standards that have been deemed to be appropriate under the security policy (see Chapter 14);
- System assurance through the application of controls for:
    - Systems development;
    - Systems operations (especially with regard to production facilities in a data center);
    - Systems integrity protection with regard to malicious software attacks from any quarter;
    - Systems use by the wider community of system business users.
- Functional testing as part of the systems development lifecycle:
    - Unit testing;
    - Integration testing;
    - System validation testing;
    - User acceptance testing;
    - Operational acceptance testing.
- Quality assurance of application systems:
    - Code reviews;
    - Coverage validation for each phase of testing.
- Penetration testing of:
    - Systems under test before release into production;
    - Operational production systems.

There are several standard frameworks available to consider for adoption. Two important ones to consider are:

1. The CobiT® Framework and
2. ISO/IEC 17799/BS 7799

### 9.5.2 Operational Risk Management Framework

The key driver for your enterprise security architecture is business risk. This section should provide detail on the management of risk within your business operations. It discusses operational risk management in general terms but constantly focuses back onto the specific needs for managing operational risk in the context of business information security.

The board of directors must define how the management of risk will be handled in general across the enterprise. Within this enterprise framework will be a description of how you will actively manage your operational risks.

The risk management framework should address:

- Risk dimension: having a hierarchical taxonomy of risks classified and grouped so as to provide a framework for risk identification;
- Enterprise organization dimension: ensuring that risk is understood and managed at every level of granularity within the enterprise organizational model;
- Process dimension: ensuring that all major process-related aspects of risk management are addressed.

The figure below shows a generic risk management process.

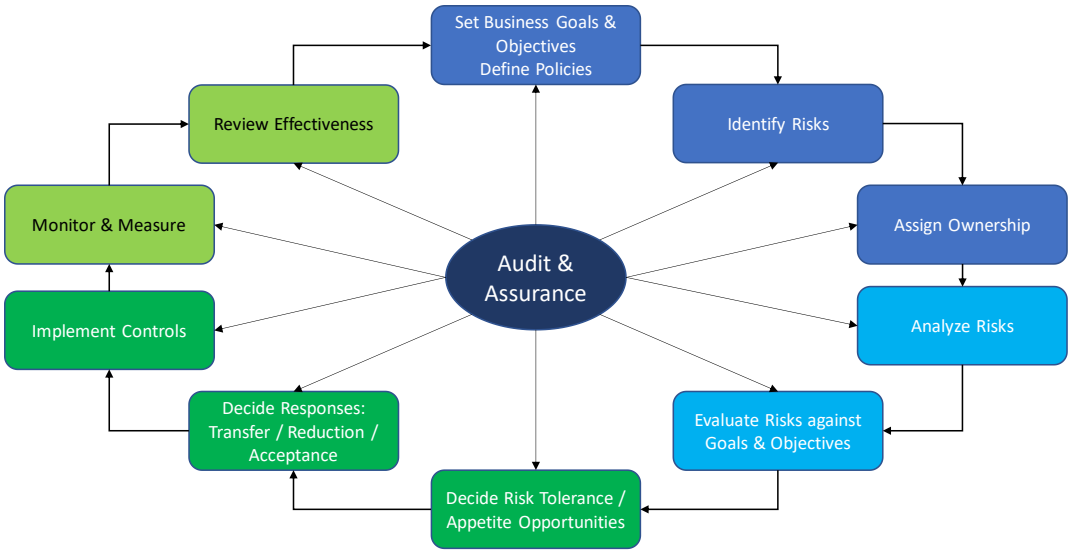


Figure 3 – Generic Risk Management Process

### 9.5.3 Security service management and support framework

The management of security services includes:

- Provisioning of security parameters and privileges for users;
- Provisioning of security parameters for application systems;
- Provisioning of security parameters for embedded systems in equipment such as routers;
- Routine security operations to maintain the corporate systems in a state of compliance with security policy and standards;
- Security monitoring and intrusion detection to detect security incidents and collect information relevant to the problem management process;
- Security incident and problem management to recover and restore secure operations following a security incident. Stages include:
    - Reporting;
    - Confirmation;
    - Escalation;
    - Response;
    - Recovery;
    - Analysis and lessons learned.
- Some help desk functions to support users with respect to their interaction with the security of corporate systems, especially to resolve security-related operational user problems;
- Managing the accounting for security-related services, such as registration and certification services;
- Security vulnerability research:
    - Collecting, collating and analyzing CERT advisory notices;
    - Intrusion testing (penetration testing);
    - Internet intelligence gathering (who is talking about us on the net and what are they planning?)

### 9.5.4 Application and user management and support framework

This section addressed one of the principal goals of any information security program must to ensure that everyone understands that information security is part of everyone's responsibility. There are several operational measures that will help you to reach this objective:

- Make sure that information security responsibility is mentioned appropriately in every job description and every contract of employment and include confidentiality agreements in contracts of employment;
- Relate this personal responsibility to the real corporate risks and ensure that each person understands the part they play as part of the wider community of staff;
- Reinforce this message of personal responsibility by direct reference to it in the corporate information security policy;
- Introduce these concepts at the earliest possible opportunity – at recruitment interviews and staff induction meetings;
- Provide adequate training and education to ensure that all employees are fully aware of their personal responsibilities and also trained in the techniques that they need to apply in their work so as to fulfil these responsibilities;
- Monitor the compliance stance and attitude of everyone throughout their employment, and use appraisal reviews to draw attention to both shortcomings and successes in the fulfilment of these responsibilities;
- Provide mandatory operational procedures for reporting security incidents of all types and ensure that all employees are aware of their duty to make such reports and that they know the mechanisms by which the reports are submitted;
- If necessary, for special types of event you may wish to provide an anonymous whistle-blowing facility to protect an employee from intimidation by a more senior and powerful person who may be abusing that power.

### 9.5.5 Security management framework sites, networks, and platforms

This section would address managing physical, network, and platform security.

Physical security depends upon the effective definition of security perimeters and the control of access both in and out of those secure areas enclosed within the perimeters.

These perimeters include managing:

- Site perimeters;
- Building perimeters;
- Internal perimeters of secure areas where sensitive processing activity or secure storage takes place;
- Locked cabinets, storage cupboards, equipment rooms and storerooms.

There are a number of additional operational controls (over and above those such as change control and capacity planning already described elsewhere in this chapter for generic operational security) that are required to ensure that data networking remains secure.

These include managing:

- Segregation of responsibilities and activities for network operations from those associated with computer systems operations;
- Clear responsibilities and operating procedures for the operation of remote networking equipment;
- Clear responsibilities and operating procedures for cryptographic key management where cryptographic networking equipment has been deployed.

Asset management and configuration management should also be addressed from a security aspect.

### 9.5.6 Framework for managing the security operations schedule

Managing the security operations schedule should encompass items such as scheduling:

- Requirements and constraints, including interdependencies between systems and earliest or latest start times to harmonize with business deadlines and cut-offs,
- Required capacity is available when the time arrives,
- maintenance programs,
- replacement of worn parts and consumables,
- repair of faults, and
- retirement and disposal at the end of useful life.