Interested in learning more about security?

SANS Institute InfoSec Reading Room

Security Controls in Service Management

Integration of security best practices into service management best practices processes enables the organization to lower the overall cost of maintaining acceptable security levels, effectively manage risks and reduce overall risk levels. This document describes an integrated approach to implementing ISO 27001/2 security best practices in an Information Technology Infrastructure Library (ITIL) v3 based service management infrastructure by identifying specific security controls in the ITIL service management framework t...

Security Controls in Service Management

GIAC G7799 Gold Certification

Author: K V Warren, warrenkat@gmail.com
Advisor: Egan Hadsell

Accepted: December 17, 2010

Abstract

Integration of security best practices into service management best practices processes enables the organization to lower the overall cost of maintaining acceptable security levels, effectively manage risks and reduce overall risk levels. This document describes an integrated approach to implementing ISO 27001/2 security best practices in an Information Technology Infrastructure Library (ITIL) v3 based service management infrastructure by identifying specific security controls in the ITIL service management framework that meet the control objectives laid out in ISO 27001 and ISO 27002. To provide more specific guidance, recommendations identified in "Twenty Critical Controls for Effective Cyber Defense: Consensus Audit" (CAG) v2.3 (SANS, 2009) are referenced in the description of each security control.

1. Introduction

The Information Technology Infrastructure Library (ITIL) v3 Core describes best practices for all aspects of the service management lifecycle. The ITIL Core consists of five publications, each providing guidance on a specific phase in the service management lifecycle. The ITIL Core publications are as follows:

- Service Strategy (2007)
- Service Design (2007)
- Service Transition (2007)
- Service Operation (2007)
- Continual Service Improvement (2007)

ISO 27001/2 (2005) and ITIL v3 are very complementary. The purpose of both standards is to identify best practices. ITIL is focused on service management best practices. ISO 27001 and ISO 27002 are focused on information security best practices. Both are based on the Plan-Do-Check-Act (PDCA) model.

From an ITIL perspective, most of the security controls identified in ISO 27001/2 are already part of service management. ITIL specifically references ISO 27001 and the requirement for an Information Security Management System.

ISO 27002 defines a control as a means to manage risk in order to satisfy the specific security objectives of the organization. Controls are also referred to as safeguards or countermeasures. ITIL defines a control as a means of managing a risk, ensuring that a business objective is achieved, or ensuring that a process is followed. Both ITIL and ISO 27001/2 identify the requirement to build security into all aspects of the service in order to effectively manage risks in the infrastructure.

Service Design section 4.6.5.1 states that "…security is not a step in the lifecycle of services and systems and that security cannot be solved through technology. Rather, information security must be an integral part of all services and systems and is an ongoing process that needs to be continuously managed using a set of security controls.

Author Name, email@address

… (security) controls will be considerably more cost-effective if included within the design of all services"

ISO 27002 section 0.2 states that "The security that can be achieved through technical means is limited, and should be supported by appropriate management and procedures. … Information security management requires, as a minimum, participation by all employees in the organization. It may also require participation from shareholders, suppliers, third parties, customers or other external parties."

As most organizations today utilize some or all of the ITIL methodologies to manage information technology services, it is beneficial to leverage the ITIL methodologies in place in the organization to ensure that security is embedded in all aspects of service management.

As ISO 27001/2 is a framework and provides general guidance, applicable critical controls identified in the CAG are also referenced in the description of each security control.

Although PCI DSS compliance is out of the scope of this paper, "PCI Compliance" (Chuvakin & Williams, 2010) is also a good source for security best practice guidance on many of the security controls identified in this paper.

The subsequent sections in this paper describe ISO 27001/2 based security controls which align with ITIL processes in each of the five service lifecycle phases.

Author Name, email@address

2. Roles and Responsibilities

Clearly defined roles and responsibilities are a critical component of effective policies, processes and procedures. ISO 27002 section 8.1.1 identifies the definition and documentation of the security roles and responsibilities of employees, contractors and third party users as a security control. ITIL identifies the requirement for clearly defined roles and responsibilities in every process in the service lifecycle.

Example: Policy

Role	Responsibility
Policy Owner	– maintain policy document – obtain executive approval for all changes to policy – publish policy – ensure awareness
Policy Review Committee	– periodically review policy – measure compliance – recommend improvements as required
Employees, Contractors and Third Parties	– act in compliance with policy

Example: Process

Role	Responsibility
Process Owner	– approve process – ensure compliance with process, ensure compliance monitored
Process documentation owner	– maintain documentation, obtain approval for all changes, publish documentation
Process review committee	– periodically review policy, measure compliance, identify improvements as required
Custodians (operational control of devices, applications)	– act in compliance with process
Employees, Contractors and Third Parties	– act in compliance with process

Author Name, email@address

References

Standard	Section
ITIL v3	Service Strategy: 6 Strategy and organization
	Service Design: 6.4 Roles and Responsibilities
	Service Transition: 6 Organizing for Service Transition
	Service Operation: 6 Organizing for Service Transition
	Continual Service Improvement: Organization for Continual Service Improvement
ISO 27001	5.1 Management commitment
ISO 27002	8.1.1 Roles and responsibilities

3. Service Strategy

Service Strategy is concerned with defining the organization's business objectives for new or existing services.

There are a number of factors which determine the success or failure of a service strategy. These factors determine those service assets which are required for the successful execution of a service strategy.

In determining a service strategy, the following security considerations should be addressed:

- Availability requirements
- Capacity requirements
- Business and IT service continuity requirements
- Compliance with legal, regulatory & contractual requirements
- Protection of service and service related assets from unacceptable risk levels
- Ensuring that all access to the service and associated assets is authorized
- Accountability for use of service and access to associated assets
- Protection of assets from unauthorized or malicious access

4. Service Design

Service Design is concerned with the design of services to meet the business objectives defined in the Service Strategy phase. Service Design is also concerned with identifying and managing risks to ensure acceptable risk levels prior to the service going live.

4.1. Information Security Management

ITIL defines the requirement for information security management as part of Service Design (see Service Design section 4.6).

4.1.1. Information Security Management System

The Information Security Management System (ISMS) identifies the requirements for the design, implementation, management and maintenance of security in the organization.

ISO 27001 defines the ISMS as "*that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security*".

ITIL specifically references ISO 27001 (Service Design section 4.6.4.3) and defines the ISMS as the "*framework of Policy, Processes, Standards, Guidelines and tools that ensures an Organization can achieve its Information Security Management Objectives*."

ISO 27001 describes the model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS). The ISMS identifies the organization's strategic direction for security and ensures that the objectives are achieved. The ISMS ensures that information security risks are appropriately managed and that information resources are used responsibly.

From an ITIL perspective, the ISMS addresses the following:

- Security Policy and supporting policies

- Security Plan – security strategy to meet business objectives as well as regulatory and contractual requirements; includes a description of all security controls
- Security organizational structure – roles and responsibilities
- Management of security risks
- Monitoring processes to ensure compliance and provide feedback on effectiveness
- Communication strategy and plan for security
- Training and awareness strategy and plan
- Identification and documentation of Security controls; operation and maintenance of the controls
- Security considerations in third party agreements/contracts
- Provisions for continuous improvement of security controls, security risk management and reduction of security risks

References

Standard	Section
ITIL v3	Service Design: Information Security Mgmt: 4.6.4.3 The Information Security Management System (ISMS)
ISO 27001	4.2.1 Establish the ISMS
ISO 27002	6.1.1 Management commitment to information security
	6.1.2 Information security co-ordination
	6.1.3 Allocation of information security responsibilities
	6.1.4 Authorization process for information processing facilities
	6.1.5 Confidentiality agreements
	6.1.6 Contact with authorities
	6.1.7 Contact with special interest groups

Author Name, email@address

4.1.2. Authorized Services/Ports/Protocols

Although neither ITIL nor ISO 27001/2 specifically identifies the requirement to restrict services, ports and protocols allowed in the network to only those which are required for the business, this is an effective control to reduce risks to the infrastructure.

Activities related to the determination of authorized services, ports and protocols are part of the scoping of the ISMS. Senior management approval of the services, ports and protocols list is highly recommended as it demonstrates management support for restricting network activity to only those services which are required to support the business functions.

Enabling only documented and approved services, ports and protocols in the network reduces the risk that an attacker could exploit an unneeded service. Software and operating systems by default typically have many services enabled which are not required by the organization. These unneeded services are often not maintained or patched by the organization.

A list of approved services should be developed for each security zone in the network and be formally approved by senior management. In addition the infrastructure should be scanned periodically to verify that there are no unauthorized services.

Diagrams showing the flow of information through the network are critical to identifying what information is flowing through the network and what services, ports and protocols are used.

Information flow diagrams are useful for gaining a good understanding of where exposures may exist in the network and where additional controls may be required. As such, information flow diagrams provide critical input to risk assessments and to the security plan. For example, information flow diagrams can be used to identify sensitive data which is being transmitted unencrypted.

Information flow diagrams clearly illustrate what required ports and protocols are in use in the network. The list of approved services for each security zone can be determined from the data gathered from these diagrams. Firewall rules and router/switch

ACLs must reflect the traffic flows identified in the information flow diagrams and the approved services list.

Event correlation and alerting tools use the list of approved services to detect anomalous activity. Vulnerability scanning tools use the list of approved services to detect unauthorized services.

References

Standard	Section
ITIL v3	Service Design: Information Security Mgmt: 4.6.4.3 The Information Security Management System (ISMS)
ISO 27001	4.2.1 Establish the ISMS
CAG (SANS)	Critical Control 4: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches - subcontrol 2, 4
	Critical Control 10: Continuous Vulnerability Assessment and Remediation - subcontrol 4
	Critical Control 13: Limitation and Control of Network Ports, Protocols, and Services – subcontrol 2
	Critical Control 15: Data Loss Prevention - Subcontrol 5

4.1.3. Risk Management Methodology and Guidelines

Risk management is concerned with the assessment and mitigation of risks to the service. The objective of risk management is to analyze security risks and weaknesses that exist in the infrastructure and that may be introduced as a result of a change.

Risk assessment is concerned with analyzing threats and weaknesses that have been or would be introduced as a result of a service change. Risk mitigation is concerned with reducing the risks related to service changes to acceptable levels.

The ISMS identifies the scope, methodology, triggers and activities for specific risk assessments related to the following processes:

ITIL Process	Risk Assessment Activity
Information Security Management	Establishing the ISMS - initial risk assessment of the service
	Monitoring and reviewing the ISMS – periodic risk assessments
Release and Deployment Management	Evaluation of risks which may be introduced by new or changed services
IT Service Continuity Management	Evaluation of risks related to service continuity in the event of a failure of a component of the service infrastructure
Availability Management	Evaluation of risks related to availability of the service
Change Management	Evaluation of risks related to Requests for Change (RFC)
Supplier Management	Evaluation of risks related to third party service providers

References

Standard	Section
ITIL v3	Service Transition: 4.6.5.9 Risk Management
	Service Design: Information Security Mgmt: 4.6.4.3 The Information Security Management System (ISMS)
	Service Design: Availability Management: 4.4.5.2 The proactive activities of Availability Management
ISO 27001	4.2.2 Implement and operate the ISMS
ISO 27002	4.1 Assessing security risks
	6.2.1 Identification of risks related to external parties
	10.1.2 Change management
	12.5.1 Change control procedures
	12.5.3 Restrictions on changes to software packages

Author Name, email@address

4.1.4. Security Policies

Security policies are security controls as they identify the organization's objectives and demonstrate support for and commitment to information security.

Security policies provide the framework for setting control objectives and controls. All individuals who interact with the service must comply with the rules and standards identified in the security policies.

A high-level security policy should be in place which identifies the organization's overall security objectives and demonstrates management commitment to security. The high-level security policy provides the basis for supporting security policies that address specific control requirements.

Supporting security policies include (but are not limited to):

- Acceptable Use Policy (Asset use, email, Internet)
- Access Control Policy
- Password Management Policy
- Log Management Policy
- Asset Disposal Policy

References

Standard	Section
ITIL v3	Service Design: Information Security Mgmt: 4.6.4.1 Security framework
	Service Design: Information Security Mgmt: 4.6.4.2 The Information Security Policy
ISO 27001	4.2.1 Establish the ISMS
ISO 27002	5.1.1 Information security policy document
	5.1.2 Review pf the information security policy
	7.1.3 Acceptable use of assets
	11.1.1 Access control policy
	11.2.1 User registration
	11.2.2 Privilege Management
	11.4.1 Policy on the use of network services

4.1.5. Data Classification & Information Handling

In order to ensure that information is appropriately protected, all information assets should be classified and the rules for handling of the information assets defined.

Information assets include directories, databases, intellectual property, documentation and test data.

The organization should define a classification schema and the criteria for each classification.

Example:

Classification	Definition
Public	Information which is intended for public consumption (e.g. public facing website
Proprietary	Not approved for general circulation outside of the organization but is unlikely to result in financial loss or serious damage to the organization's reputation
Confidential	Unauthorized disclosure would be prejudicial to the interest or reputation of the organization or be of advantage to the competition
Secret	Unauthorized disclosure could result in the inability to conduct business, severely impact the stability of the organization, or place the organization at serious competitive disadvantage

All information assets identified in the Asset Inventory (see section *5.2.1 Asset Inventory*) should be classified and appropriate handling rules and procedures defined.

For each defined classification level, the following should be defined:

- Access controls/restrictions
- Copying procedures/restrictions
- Storage procedures/restrictions
- Encryption requirements – at rest, in transit (e.g. the CAG recommends that sensitive data on laptops and on removable, easily transported storage media should be encrypted)
- Data retention requirements (e.g. on-line for three months, off-line for one year)

- Restrictions on the transmission of the information (e.g. via email, fax, regular mail)
- Restrictions on communication of the information (e.g. via phone, voicemail, etc.)
- Procedures for the destruction of the information

References

Standard	Section
ITIL v3	Service Design: Information Security Mgmt: 4.6.4.2 The Information Security Policy
	Service Design: Information Security Mgmt: 4.6.4.3 The Information Security Management System (ISMS)
ISO 27001	4.3 Documentation requirements
ISO 27002	7.2.1 Classification guidelines
	7.2.2 Information labeling and handling
CAG (SANS)	Critical Control 9: Controlled Access Based on Need to Know – subcontrol 1
	Critical Control 15: Data Loss Prevention – subcontrols 1, 6

4.1.6. Security Plan

The security plan (also called a risk treatment plan) identifies appropriate security measures for the management of information security risks in the infrastructure. The security plan is developed as part of establishment of the ISMS.

The steps in developing the security plan are:

1. Identify risks
2. Analyze and evaluate the risks
3. Identify and evaluate options for the treatment of risks
4. Select control objectives and controls for the treatment of risks

Authorized software

Authorized services, ports, protocols

The security plan should describe how each identified control is to be implemented along with the appropriate management action, resource responsibilities and priorities.

The following should be addressed in the security plan:

- Organizational structure and security related roles and responsibilities
- Security policies
- Authorized software
- Authorized services, ports and protocols
- Perimeter defence - control of connections to/from foreign networks (Internet, private links to external organizations, etc,)
- Security zoning – required controls for each zone E.g. Internet zone – low trust; operations – medium trust; data centre – high trust. Specific controls may vary for each zone.
- Boundary defence
- Control of connections between security zones. E.g. between the Internet zone and the operations zone, between the operations zone and the data centre zone
- Access controls- host based, network based
- High availability/redundancy mechanisms
- Event, health and capacity monitoring
- Audit and event logging and alerting
- Processes and procedures
- Audit controls – need mechanisms to measure the effectiveness of the security controls

The CAG identifies a number of critical security controls which should be considered in the security plan – see below.

References

Standard	Section
ITIL v3	Service Design: Information Security Mgmt: 4.6.4.1 Security framework
	Service Design: Information Security Mgmt: 4.6.5.1 Security controls
	Service Design: Information Security Mgmt: 4.6.6.2 Outputs
ISO 27001	4.2.1 Establish the ISMS
ISO 27002	4 Risk assessment and treatment
	6.1.2 Information security co-ordination
	11.4.4 Remote diagnostic and configuration port protection
	11.4.5 Segregation in networks
	11.4.6 Network connection control
	11.4.7 Network routing control
	12.1.1 Security requirements analysis and specification
CAG (SANS)	Critical Control 2: Inventory of Authorized and Unauthorized Software – subcontrol 1
	Critical Control 4: Secure Configurations for Network Devices such as Firewalls, Routers and Switches – subcontrols 2, 6
	Critical Control 5: Boundary Defense – subcontrols 1, 2, 4, 5, 6
	Critical Control 6: Maintenance, Monitoring, and Analysis of Audit Logs – subcontrol 9
	Critical Control 7: Application Software Security – subcontrol 1
	Critical Control 8: Controlled Use of Administrative Privileges – subcontrols 11, 12
	Critical Control 9: Controlled Access Based on Need to Know – subcontrols 2, 3
	Critical Control 12: Malware Defenses – subcontrols 1, 2
	Critical Control 13: Limitation and Control of Network Ports, Protocols, and Services – subcontrol 1, 3
	Critical Control 14: Wireless Device Control – subcontrols 2, 4, 8, 9, 10
	Critical Control 15: Data Loss Prevention – subcontrol 1
	Critical Control 16: Secure Network Engineering – subcontrols 1, 2, 3
	Critical Control 19: Data Recovery Capability – subcontrols 2, 3

Author Name, email@address

4.2. Capacity Management

4.2.1. Capacity Monitoring

Capacity monitoring minimizes the risk of service degradation and/or failures due to insufficient capacity. Utilization of service resources should be monitored and appropriate action taken if utilization exceeds a defined threshold (e.g. "filesystem >= 80% full"). Resources should also be monitored to ensure acceptable system performance.

Resources to be monitored include CPU utilization, memory utilization, disk usage, license usage, etc.

Most service resources can be monitored automatically using capacity and performance monitoring tools.

Mechanisms should be in place to alert when utilization of resources exceeds a defined threshold using automated tools (e.g. automatic creation of an incident ticket).

In particular, the CAG identifies the requirement to monitor the storage capacity of all systems which store log data to minimize the risk that log data is lost due to insufficient capacity.

References

Standard	Section
ITIL v3	Service Design: Capacity Management: 4.3.5.4 The underpinning activities of Capacity Management
	Service Design : Capacity Management: 4.3.5.5 Threshold management and control
ISO 27001	4.2.3 Monitor and review the ISMS
ISO 27002	10.3.1 Capacity management
CAG (SANS)	Critical Control 6 Maintenance, Monitoring, and Analysis of Audit Logs: Subcontrol 2

4.2.2. Capacity Review

The capacity of all components comprising the service should be reviewed periodically to minimize the risk of service degradation of a failure due to insufficient capacity as usage patterns change.

The capacity review evaluates current utilization and projects future capacity requirements based on expected demand for the service.

References

Standard	Section
ITIL v3	Service Design: Capacity Management: 4.3.5.7 Modelling and trending
ISO 27001	4.2.3 Monitor and review the ISMS
ISO 27002	10.3.1 Capacity management

4.3. Availability Management

4.3.1. Assessment of Risks Related to Availability

Risks related to availability should be assessed periodically to ensure that actual service availability meets or exceeds agreed-upon targets.

Availability Management, Information Security Management and IT Service Continuity Management should work together to conduct integrated risk analysis and management assessments.

The risk assessment methodologies to be used are determined jointly by Availability Management and Information Security Management.

There are a number of ways to approach assessment of risks related to availability. Information Security Management is responsible for determining the risk assessment methodology (or combination of methodologies) which best fits the organization's requirements.

ITIL v3 identifies the following risk assessment methodologies:

Risk Assessment Methodology	Description
Unavailability analysis	Analysis of the incident lifecycle (time to detect incident, diagnose, repair, recover, restore. Reduction of any of these metrics improves overall availability)
Service Failure Analysis	Identification of the underlying causes of service interruptions
Component Failure Impact Analysis	Assessment of the potential impact of component failures
Single Point of Failure analysis	Identification of the single points of failure
Fault Tree Analysis	Determination of the chain of events that causes a disruption to services
Risk assessment and management	Identification and quantification of risks and justifiable countermeasures

References

Standard	Section
ITIL v3	Service Design: Availability Management: 4.4.5.2 The proactive activities of Availability Management – page 108 Service Failure Analysis
	Service Design: Availability Management: 4.4.5.2 The proactive activities of Availability Management – page 117 Single Point of Failure analysis
	Service Design: Availability Management: 4.4.5.2 The proactive activities of Availability Management – page 117 Fault Tree Analysis
	Service Design: Availability Management: 4.4.5.2 The proactive activities of Availability Management – page 118 Risk Analysis and Management
ISO 27001	4.2.2 Implement and operate the ISMS
ISO 27002	4.1 Assessing security risks
	13.2.2 Learning from information security incidents

4.3.2. Availability Monitoring

In order to ensure that the availability of the service is not compromised by failures in the system or by security incidents, availability monitoring requirements should be determined and the identified monitoring implemented.

ISO 27002 is concerned with the confidentiality, integrity and availability of information assets. As such Availability Management and Information Security Management share the requirement to monitor availability and should work together to determine the requirements for monitoring and measurement of service and component availability.

Availability monitoring metrics include the following:

Category	Purpose	Monitoring Metrics	Response
Health	Detect failures in the system	Health of hardware, OS, applications, services, temperature, etc.	Alert on failures, errors, warnings
Performance	Detect performance issues which could negatively impact availability	Performance levels such as CPU load, memory, etc.	Alert when performance drops below acceptable levels
Capacity	Detect capacity issues which could negatively impact availability	Resource utilization such as disk, licensing, and network bandwidth utilization	Alert when performance drops below acceptable levels
Anomalous Activity	Detect anomalous activity which could negatively impact availability and/or the security of the system	Anomalous activity signatures (intrusion detection), unusual login activity, virus detection, configuration changes	Alert on anomalous activity

Author Name, email@address

References

Standard	Section
ITIL v3	Service Design: Information Security Mgmt: 4.6.6 Triggers, inputs, outputs and interfaces
	Service Design: Information Security Mgmt: 4.6.6.2 Outputs
	Service Design: Information Security Mgmt: 4.6.9 Challenges, Critical Success Factors and risks
	Service Design: 4.4 Availability Management
ISO 27001	4.2.4 Maintain and improve the ISMS
ISO 27002	10.10.5 Fault Logging
	13.1.1 Reporting information security events
	13.2.1 Responsibilities and procedures
	13.2.2 Learning from information security incidents

4.4. Service Level Management

4.4.1. Security Related Service Level Targets

Business requirements may warrant separate service level requirements (SLRs) and service level agreements (SLAs) for incidents resulting from anomalous activity ("security incidents"). In this case the anomalous activity related SLOs may be more stringent than for SLAs related to failures in the system.

In order to measure security incidents separately from incidents related to failures in the system, the criteria for a "security incident" must be defined. It is useful to mark the incident ticket in some way to facilitate sorting of tickets into security and non-security related.

As for other types of incidents, mechanisms should be in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.

References

Standard	Section
ITIL v3	Service Design: Information Security Mgmt: 4.6.6 Triggers, inputs, outputs and interfaces
	Service Design: Information Security Mgmt: 4.6.6.2 Outputs
	Service Design: 4.2 Service Level Management
ISO 27001	4.2.3 Monitor and review the ISMS
ISO 27002	13.2.2 Learning from information security incidents

4.5. IT Service Continuity Management

4.5.1. Service Continuity Management Process

Both ITIL and ISO 27002 identify the requirement to minimize the impact of component failures or disasters on critical services and to ensure timely resumption of these services.

Information security requirements should be identified and included in the Service Continuity Management process. From a security perspective the Service Continuity Management process should include:

- Assessment of service continuity risks – likelihood and impact of failures, impact of failures
- Identification of all assets involved in critical business processes
- Identification and consideration of implementation of additional preventive and mitigating controls
- Ensuring the safety of personnel and the protection of information processing facilities and organizational property
- Development and documentation of business continuity plans which address information security requirements
- Regular testing and updating of the plans and processes in place
- Ensuring that the management of business continuity is incorporated into the organization's processes and structure
- Ensuring that responsibility for the business continuity management process is assigned at an appropriate level within the organization

References

Standard	Section
ITIL v3	Service Design: 4.5 IT Service Continuity Management
ISO 27001	4.2.1 Establish the ISMS
ISO 27002	14.1.1 Including information security in the business continuity management process
CAG (SANS)	Critical Control 19: Data Recovery Capability – subcontrol 1

4.5.2. Service Continuity Risk Assessment

Service continuity risk assessments should include security considerations to ensure that acceptable security levels are maintained in the event of a failure.

Service continuity risk assessments are focused on the identification and assessment of events that could cause interruptions to business processes.

Event scenarios include equipment failure, human error, theft, fire, natural disasters and acts of terrorism.

Each identified risk should be assessed to determine the probability and impact of identified events.

The ISMS should include determination of appropriate risk assessment methodologies and determination of the scope of specific risk assessment activities for different failure scenarios (see section *4.1.3 Risk Management Methodology and Guidelines*).

References

Standard	Section
ITIL v3	Service Design: IT Service Continuity Management: 4.5.5.2 Stage 2 – Requirements and strategy
ISO 27001	4.2.1 Establish the ISMS
ISO 27002	14.1.2 Business continuity and risk assessment

4.5.3. Service Continuity Plans

Both ITIL and ISO 27002 identify the requirement for Service Continuity plans to ensure that services can be resumed within an acceptable timeframe.

ISO 27002 identifies the requirement for a single framework of service continuity plans to ensure that information security requirements are consistently addressed.

Note that the scope of ISO 27002 includes business processes outside of IT (business continuity). ITIL is focused specifically on IT management (service continuity).

Service Continuity Plans should include:

- Identification of all roles and responsibilities
- Identification of service continuity procedures
- Implementation of business continuity procedures
- Operational procedures to follow during recovery and restoration of services
- Documentation of processes and procedures
- Education of staff on the service continuity processes and procedures
- Provision for testing and updating the service continuity plans

References

Standard	Section
ITIL v3	Service Design: IT Service Continuity Management: 4.5.5.2 Stage 3 – Implementation
ISO 27001	4.2.1 Establish the ISMS
ISO 27002	14.1.3. Developing and implementing continuity plans including information security
	14.1.4 Business continuity planning framework

4.5.4. Testing of Service Continuity Plans

Both ITIL and ISO 27002 identify the requirement for periodic testing of Service Continuity plans to ensure that service continuity plans are up to date and effective

Service Continuity testing includes a variety of techniques including:

- Desktop – identify scenarios and review recovery and resolution plans
- Simulations
- Technical recovery testing – e.g. recover from backup tapes
- Recovery at an alternate site (as applicable)
- Supplier facilities and services – ensure that third parties will meet service level commitments
- Complete rehearsals – test all components of the service continuity plan to ensure that the organization can cope with interruptions

References

Standard	Section
ITIL v3	Service Design: IT Service Continuity Management: 4.5.5.2 Stage 3 – Implementation
ISO 27001	4.2.2 Implement and operate the ISMS
ISO 27002	14.1.5 Testing, maintaining and re-assessing business continuity plans
CAG (SANS)	Critical Control 4: Secure Configuration for Network Devices – subcontrol 3
	Critical Control 18: Incident Response Capability – subcontrol 6

4.6. Supplier Management

4.6.1. Security Requirements Identified in Third Party Agreements

In order to maintain the security of the organization's information and services that are accessed, processed, communicated to or managed by external parties, the organization's security requirements should be identified in third party agreements.

Contracts with external parties should ensure that suppliers are in conformance with the organization's business objectives and security policies.

Third party agreements should include provision for mechanism(s) to periodic evaluate conformance (e.g. periodic audit of supplier)

Risks related to third parties should be assessed (see section *4.1.3 Risk Management Methodology and Guidelines*) and appropriate controls implemented before granting access.

Mechanisms to periodically assess risks related to suppliers and evaluate supplier conformance should be established.

References

Standard	Section
ITIL v3	Service Design: Information Security Mgmt: 4.6.6 Triggers, inputs, outputs and interfaces
	Service Design: 4.7 Supplier Management
ISO 27001	4.2.1 Establish the ISMS
ISO 27002	6.2.1 Identification of risks related to external parties
	6.2.2 Addressing security when dealing with customers
	6.2.3 Addressing security in third party agreements
	10.2.1 Service delivery
	10.2.2 Monitoring and review of third party services
	10.2.3 Managing changes to third party services

5. Service Transition

Service Transition is concerned with ensuring that changes introduced into the infrastructure are managed in a consistent and effective manner. Service Transition is also concerned with ensuring that unacceptable risks are not introduced into the infrastructure as a result of a change. To ensure consistency and acceptable risk levels, information about assets and configurations must be kept current and accurate so that effective decisions can be made about changes.

In addition, Service Transition is concerned with ensuring that the ongoing management and support of the service requirements meet the requirements specified in Service Design.

Author Name, email@address

5.1. Release & Deployment Management

5.1.1. Risk Assessment of Proposed Releases

Assessing security risks related to proposed releases enables the organization to identify and mitigate any unacceptable risks before being introduced into the system.

Assessment of risks should be completed early in the Release phase so that appropriate mitigation can be built into the Release plan.

If the proposed release includes the use of a service provided by a third party, the risks related to the third party's service should be considered.

The risk assessment of a proposed release should take into consideration the use and handling of test data. Test data used for the evaluation of a new release should be protected and controlled – test data should be appropriately labeled and handled in accordance with the organization's data classification and information handling policies.

As part of the risk assessment activity, a report is prepared which includes a summary of findings along with recommendations for the mitigation unacceptable risks. Change approval should be dependent on implementing the recommended mitigation as part of deployment of the release.

References

Standard	Section
ITIL v3	Service Transition: Evaluation: 4.6.5.9 Risk Management
	Service Design: Information Security Mgmt: 4.6.4.3 The Information Security Management System (ISMS)
	Service Design: Availability Management: 4.4.5.2 The proactive activities of Availability Management
ISO 27001	4.2.2 Implement and operate the ISMS
ISO 27002	4.1 Assessing security risks
	6.2.1 Identification of risks related to external parties
	12.1.1 Security requirements analysis and specification
	12.4.2 Protection of system test data
	12.5.5 Outsourced software development

Author Name, email@address

5.2. Asset & Configuration Management

5.2.1. Asset Inventory

An accurate and current inventory of organizational assets is required in order to ensure that appropriate protection of the assets can be identified and implemented. ISO 27001 defines an asset as anything that has value to the organization.

ITIL identifies the following asset types:

- Management
- Organization
- Process
- Knowledge
- People
- Information
- Applications
- Infrastructure (equipment, environmental, etc.)
- Financial Capital

ISO 27002 identifies the same asset types plus intangible assets such as the reputation and image of the organization. Both ITIL and ISO 27002 identify the requirement to clearly identify all assets and maintain an inventory of assets.

The asset inventory is part of the ITIL Configuration Management System. Note that the asset inventory and the Configuration Management System are themselves assets.

Every identified asset should have a clearly defined owner. The asset owner is responsible for ensuring that information and assets are appropriately classified and defining and periodically reviewing access restrictions and classifications in alignment with applicable access control policies.

Asset information will vary with the type of asset. One of the activities in Asset and Configuration Management activities is to identify required asset information.

Asset information examples:

Asset	Asset Information
Network device	Hostname
	Owner
	IP Address(es)
	Make and Model
	Support Contract
	Version & Patch Level
	Serial Number
	Record of changes to asset
Process/Procedure/Policy Documents	Location & file name
	Owner
	Classification
	Version
	Release date of current version

Author Name, email@address

References

Standard	Section
ITIL v3	Service Design: Information Security Management: 4.6.4.3 The Information Security Management System (ISMS)
	Service Transition: Service Asset and Configuration Management: 4.3.1 Purpose, goal and objective
	Service Transition: Service Asset and Configuration Management: 4.3.3 Value to business
	Service Transition: Service Asset and Configuration Management: 4.3.4.2 Basic concepts
	Service Transition: Service Asset and Configuration Management: 4.3.4.3 Configuration Management System
	Service Transition: Service Asset and Configuration Management: 4.3.5.3 Configuration identification
ISO 27001	4.2.1 Establish the ISMS
ISO 27002	7.1.1 Inventory of assets
	7.1.2 Ownership of assets
CAG (SANS)	Critical Control 1: Inventory of Authorized and Unauthorized Devices – subcontrol 2, 5
	Critical Control 2: Inventory of Authorized and Unauthorized Software – subcontrol 1

5.2.2. Asset Review

An accurate and current inventory of organizational assets and asset information is required in order to ensure that appropriate protection of the assets can be identified and implemented.

The objectives of the Asset Review are to ensure that the information asset information (configurations, ownership, status, location, etc.) contained in the asset inventory is complete and that the asset information contained in the asset inventory conforms to actual asset information and to verify the physical existence of assets in the organization.

The first step in the Asset Review is to conduct an inventory of all assets and reconcile the actual assets to the asset inventory. The next step is to conduct a review of

actual asset information and reconcile it against the information contained in the asset inventory repository. The final steps are to prepare a report on all deficiencies in the asset inventory and submit a request for change to correct the deficiencies in the asset inventory.

Asset Reviews are typically conducted yearly or are triggered as a result of an incident which may have occurred directly or indirectly as a result of errors in the inventory repository. For example a change to a device results in a failure due to incorrect information about the device such as OS version or IP address.

References

Standard	Section
ITIL v3	Service Design: Information Security Management: 4.6.4.3 The Information Security Management System (ISMS)
	Service Transition: Service Asset and Configuration Management: 4.3.1 Purpose, goal and objective
	Service Transition: Service Asset and Configuration Management: 4.3.3 Value to business
	Service Transition: Service Asset and Configuration Management: 4.3.5.6 Verification and audit
ISO 27001	4.2.3 Monitor and review the ISMS
ISO 27002	7.1.1 Inventory of assets
	7.1.2 Ownership of assets

5.2.3. Secure Baselines

Secure Baselines reduce the risk of a device or application compromise in the event that other network and/or perimeter defenses are breached by ensuring that the organization's security policies are enforced.

A secure baseline configuration should be developed for each component type. Secure baselines should be applied as part of the initial build of the component.

A risk assessment of each component type is recommended to determine what actual risks exist. Port scans and vulnerability scans are very useful in determining actual risks.

If there is no business justification for running a service on a device then the service should be disabled or removed completely from the device. All functionality which is non-compliant with the organization's security policies should be disabled. For example, if the organization's password policy states that password credentials are not transmitted or stored in clear text then services such as telnet and FTP must be disabled.

Where possible, use access control configuration templates which are in compliance with the organization's security policies. User and group templates should grant minimum access rights and privileges needed for the user to perform his/her job function. The user templates should enforce the organization's password policy (expiry, lifetime, minimum length, complexity, difficulty, lockout after X failed attempts, etc).

Baseline configurations should specify the current version and patch levels supported by the organization.

Logging should be enabled and the appropriate logging levels configured as per the organization's log management policy. Log data to be collected includes user login activity, access to services and resources, device and application faults, configuration changes and anomalous activity in the network.

Most device and application vendors provide security hardening guidelines to assist the organization in hardening their products.

Secure baseline configurations should be documented, tested and maintained for each component type deployed in the infrastructure.

Author Name, email@address

Information Security Management is responsible for ensuring that secure baselines meet the organization's security policies and risk treatment plans.

To ensure that secure baselines are implemented and tested when new components are deployed in the infrastructure, additional steps in the Release Management, Change Management and Information Security Management processes are required.

Release Management is responsible for identifying any requirements for exceptions to the approved secure baseline configuration and, if so, identify any mitigating controls and obtain management approval. Release Management is also responsible for ensuring that secure baseline configurations are verified.

Change Management is responsible for ensuring that the secure baseline configuration has been applied to any new components and tested prior to deployment in production.

Information Security Management is responsible for ensuring that secure baseline configurations are defined and tested.

References

Standard	Section
ITIL v3	Service Transition: Configuration Management 4.3.5.3 Configuration identification – page 77 Identification of configuration baselines
ISO 27001	4.2.2 Implement and operate the ISMS
ISO 27002	10.6.1 Network controls
	10.10.1 Audit logging
	11.3.1 Password use
	11.4.1 Policy on use of network services
	11.5.1 Secure log-on procedures
	11.5.5 Session time-out
	11.5.6 Limitation of connection time
	12.1.1 Security requirements analysis and specification
	12.4.1 Control of operational software
	12.6.1 Control of technical vulnerabilities
CAG (SANS)	Critical Control 3: Secure Configurations for Hardware and Software on Laptops, Workstations and Servers – subcontrols 1, 2, 3, 5
	Critical Control 4: Secure Configuration for Network Devices such as Firewalls, Routers, and Switches – subcontrols 1, 2
	Critical Control 6: Maintenance, Monitoring, and Analysis of Audit Logs – subcontrols 1, 2
	Critical Control 8: Controlled Use of Administrative Privileges – subcontrols 1, 2, 3, 4, 5, 8
	Critical Control 11: Account Monitoring and Control – subcontrol 4
	Critical Control 12: Malware Defenses – subcontrols 3, 4
	Critical Control 14: Wireless Device Control – subcontrols 1, 5, 6, 11, 12

Author Name, email@address

5.2.4. Clock Synchronization

Both ITIL and ISO 27002 have a requirement for all devices and applications to be synchronized to a reliable and accurate time source. Synchronized clocks are essential for investigating events across multiple systems in the infrastructure.

If system clocks are not synchronized it may be difficult to determine whether two events are related. For example an event on one system triggers a failure on second system but the clock on the first system is behind. In this case the event that triggered the failure will appear to have occurred after the failure.

Clock synchronization is particularly important for audit log data. Accurate timestamps on audit log data is critical for troubleshooting, for event correlation and for use as evidence in legal or disciplinary cases.

Clock synchronization is typically achieved by configuring all devices to periodically (e.g. every 15 minutes) synchronize their clocks to the same reliable time sources using the network time protocol (NTP). The CAG recommends implementing at least two synchronized time sources which all devices in the network retrieve the time from.

Clock synchronization configurations should be included in the Secure Baseline configuration.

References

Standard	Section
ITIL v3	Service Transition: Service Asset and Configuration Management: 4.3.5.3 Configuration identification
	Service Operation : Event Management : 4.1.5.6 Event correlation
ISO 27001	4.2.2 Implement and operate the ISMS
ISO 27002	10.10.6 Clock synchronization
CAG (SANS)	Critical Control 6: Maintenance, Monitoring, and Analysis of Audit Logs – subcontrol 7

5.2.5. Configuration Control

Both ITIL and ISO 27002 identify the requirement to maintain a record of configurations over time. Several ITIL processes are dependent on historical configuration data.

Incident Management uses configuration backups to restore systems to a known good configuration after a failure or compromise.

Problem Management uses historical configurations to determine root cause of problems. If a compromise of a system occurs, the current configuration can be compared to the last known good configuration as part of an investigation to determine how the compromise occurred. If a system becomes unstable, the current configuration may be compared to the last known good configuration to determine what has changed as part of the investigation into root cause.

Release and Deployment Management uses current configurations to plan for new releases. For example, in preparation for deployment of a software upgrade a copy of the current configuration is applied in the lab, the upgrade is applied, and then the system is verified.

Information Security Management uses configuration data for assessing risks in the infrastructure.

Each time a configuration change is applied to a component, a copy of the configuration should be retained. The configuration copy should be labeled with the date the configuration was pulled from the component.

The mechanism used to copy a configuration will vary with the type of component. Network devices typically have a built-in tool to "dump" the configuration. This dump can also be used to restore the configuration.

Software backup tools are often used to make copies of operating systems and applications but a separate backup of the configuration outside of any normally scheduled backups is useful as a configuration "snapshot". All information related to configuration backups (location, date & time of backup, name of backup) of an asset should be recorded in the configuration management system.

Discovery tools are also available which can extract configuration details from a system or application.

References

Standard	Section
ITIL v3	Service Design: Information Security Management: 4.6.4.3 The Information Security Management System (ISMS)
	Service Transition: Service Asset and Configuration Management: 4.3.1 Purpose, goal and objective
	Service Transition: Service Asset and Configuration Management: 4.3.3 Value to business
	Service Transition: Service Asset and Configuration Management: 4.3.4.3 Configuration Management System
	Service Transition: Service Asset and Configuration Management: 4.3.5.4 Configuration control
ISO 27001	4.2.2 Implement and operate the ISMS
ISO 27002	10.1.2 Change management
	13.2.1 (Management of information security incidents and improvements) Responsibilities and Procedures
	12.5.1 Change control procedures
CAG (SANS)	Critical Control 4: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches – subcontrol 4

5.2.6. Verification of Actual Configurations

The last known good configuration is a snapshot of the configuration at a time where the configuration has been tested and determined to be in a good state. For example a configuration may be determined to be in a good state at the time that the component is deployed. The configuration at the time of the last security testing (e.g. vulnerability scans and/or penetration tests, audit review, etc.) may be determined to be a known good configuration. The secure baseline may also be considered to be the known good configuration.

Actual device and application configurations should be periodically compared to the last known good configuration and all deviations should be justified in order to ensure

that unexpected risks are not introduced into the infrastructure, ensure that configurations are in compliance with the organization's security policies and ensure compliance with change management policies.

An ad hoc review of actual device and applications configurations against the last known good configuration is important when a breach attempt is suspected or has occurred in the infrastructure. Any deviations should be identified and addressed promptly to limit any potential damage. Of particular interest are configuration items such as user rights/privilege changes, changes to automatically started processes (new process, process not longer started by system, etc.) and changes to files.

Actual configurations should be reconcilable to either the Baseline Configuration, an approved Request for Change or to an approved Request for Exception.

References

Standard	Section
ITIL v3	Service Design: Information Security Management: 4.6.4.3 The Information Security Management System (ISMS)
	Service Transition: Service Asset and Configuration Management: 4.3.5.4 Configuration control
ISO 27001	4.2.2 Implement and operate the ISMS
ISO 27002	10.1.2 Change management
	12.5.1 Change control procedures
CAG (SANS)	Critical Control 4: Secure Configuration for Network Devices such as Firewalls, Routers, and Switches –subcontrol 1

5.3. Service Validation & Testing

5.3.1. Security Acceptance Testing

Both ITIL and ISO 27002 identify the requirement to verify changes prior to implementation in production to ensure compliance with the organization's requirements. This includes verifying that the change will not introduce unacceptable risks into the infrastructure.

Information Security Management is responsible for determining what security testing is required depending on the nature and scope of the proposed change.

Security acceptance tests for applications, operating systems and network operating systems should include penetration testing, vulnerability scans and/or port scans.

Penetration testing tools effectively simulate an attack from a malicious source. These tools perform an active analysis of the system for any potential vulnerabilities in the network due to improper system configuration, software flaws, or weak technical countermeasures.

Vulnerability scanners probe remote systems and reports on vulnerabilities. Vulnerability scanners use signatures for known vulnerabilities to detect vulnerabilities in the target system.

Port scanners probe remote devices for open ports. Port scans are useful for identifying any ports/services which should not be active.

Many tools, both commercial and public domain, are available which are capable of executing multiple types of security testing.

For applications, security acceptance tests should include input data validation, output data validation, validation of the authenticity and protection of message integrity and testing for data leakage.

Input validation reduces the risk of system and/or data compromise by invalid data input (out-of range values, invalid characters, etc.) Applications should verify all data inputted into the system before processing it. Commercial and freeware input data validation tools are available.

Output data validation helps to ensure that the processing of stored information is correct and appropriate. Typically, output data validation is addressed in functional acceptance testing. However from a security perspective, the protection of the information also needs to be considered. Access controls must be in place and verified to protect the information. For example if only certain people are authorized to access

certain information (e.g. financial data) then it is important to verify that no one else can access that information.

Validation of the authenticity and protection of message integrity ensures that applications can detect any corruption of information due to processing errors or deliberate acts. Ideally applications should be designed with appropriate controls built-in such as logging all data modification activities (insertions, deletions, modifications). Validation activities include modifying data and ensuring that all data modification activities are logged (who, what, when).

It is important to ensure that information about the system is not inadvertently leaked. For example, default login screens may reveal information about the system (product, version, etc.) that an intruder could use to exploit and compromise the system.

References

Standard	Section
ITIL v3	Service Transition: Service Validation and Testing: 4.5.4.10 Types of testing – Table 4.2 Examples of Service Management manageability tests
ISO 27001	4.2.2 Implement and operate the ISMS
ISO 27002	10.3.2 System acceptance
	12.2.1 Input data validation
	12.2.2 Control of internal processing
	12.2.3 Message Integrity
	12.2.4 Output data validation
	12.5.4 Information leakage
CAG (SANS)	Critical Control 7: Application Software Security – subcontrol 3
	Critical Control 8: Controlled Use of Administrative Privileges – subcontrol 2

5.4. Change Management

The objective of Change Management from both an ITIL and ISO 27002 perspective is to minimize risks (business and security) related to changes.

5.4.1. Change Approval

For both ITIL and ISO 27002 change approval is a critical audit control to ensure that changes do not introduce unacceptable risks into the infrastructure.

Organizations may have separate approval processes depending on the type of change. For example the approval process for requests for service might include the requester's management approval while changes to the infrastructure are approved by the change advisory board. Regardless of how the change is categorized, if the change has the potential to negatively affect the security of the infrastructure then security related activities need to be included in the change process.

From a security perspective, each proposed change should be evaluated to determine if a security assessment is required

The Change Manager evaluates each Request for Change (RFC) and approves or rejects the RFC based on a number of factors such as the results from business impact assessments, risk assessments and pre-change functional and security verification testing. As well, the completeness and accuracy of the change implementation plan including backout plans and post change functional and security verification test plans should be considered.

It is also important to consider other changes being implemented in the infrastructure (e.g. two proposed changes determined to be low risk may have much higher risk if implemented at the same time).

References

Standard	Section
ITIL v3	Service Design: Information Security Mgmt: 4.6.6 Triggers, inputs, outputs and interfaces
	Service Transition: 4.2 Change Management
ISO 27001	4.2.2 Implement and operate the ISMS
ISO 27002	10.1.2 Change management
	12.5.1 Change control procedures
	12.5.2 Technical review of applications after operating system changes
	12.5.3 Restrictions on changes to software packages

5.4.2. Risk Assessment of Proposed Changes

Risks to availability of the service and/or the security of the service should be assessed prior to approval of a RFC.

A complex change that has not been implemented before which would require significant time to backout if a problem occurs might be considered high risk. A simple change that has been implemented successfully previously in the infrastructure might be considered low risk.

A change that may introduce new vulnerabilities into the infrastructure or increase the risk of exploitation of existing vulnerabilities might be considered high risk.

Information Security Management plays a role in the assessment of every change. In particular Information Security Management is concerned with ensuring that appropriate risk assessments are executed prior to approval of a proposed change.

The ISMS should include determination of appropriate risk assessment methodologies and the scope of specific risk assessment activities for different types of changes (see section *4.1.1 Information Security Management System).*

References

Standard	Section
ITIL v3	Service Transition: 4.2 Change Management
	Service Design: Information Security Mgmt: 4.6.4.3 The Information Security Management System (ISMS)
	Service Design: Information Security Mgmt: 4.6.6 Triggers, inputs, outputs and interfaces
ISO 27001	4.2.2 Implement and operate the ISMS
ISO 27002	4.1 Assessing security risks
	6.2.1 Identification of risks related to external parties
	10.1.2 Change management
	12.5.1 Change control procedures
	12.5.3 Restrictions on changes to software packages

5.4.3. Update Log Management System

Log data provides valuable input to the ITIL Event Management process and the collection and retention of log data is a requirement for ISO 27002.

The organization's log management policy identifies the logging requirements and minimum log data retention periods (e.g. three months online, one year off-line).

Change implementation plans should include steps to configure collection of device and application log data (audit logs, configuration changes, error logs, etc.) as applicable. This reduces the risk of loss of log data due to failure to configure log generation and retention on new devices and applications.

Log data should be stored in such a way that it cannot be tampered with in order to ensure the integrity and completeness of log data. Note that in most cases device and application local log data repositories cannot be protected from tampering.

References

Standard	Section
ITIL v3	Service Transition: Change Management: 4.2.6 Process activities, methods and techniques
ISO 27001	4.2.2 Implement and operate the ISMS
ISO 27002	10.10.1 Audit logging
	10.10.3 Protection of log information
	10.10.4 Administrator and operator logs
	10.10.5 Fault logging

5.4.4. Update Configuration Management Database (CMDB)

All change implementation plans should include a step to update the Configuration Management DataBase (CMDB) as applicable to reflect what has changed on all affected systems.

The CMDB contains information about configuration items (CIs) which is used by other procedures and processes. As asset information contained in the CMDB supports other processes, it is critical that asset configuration is kept current and accurate.

The version and patch level of devices and applications is of interest to Problem Management for ensuring that system patching is kept current.

Incident detection and response is dependent on information about component function, purpose, IP address, hostname, owner, configuration, etc.

Configuration and Asset Management processes rely on current and accurate information in the asset inventory.

Risk assessments are dependent on the information about devices and applications in the CMDB, particularly version and patch levels of components.

References

Standard	Section
ITIL v3	Service Transition: 4.2 Change Management
	Service Transition: Service Asset and Configuration Mgmt: 4.3.1 Purpose, goal and objectives
ISO 27001	4.2.2 Implement and operate the ISMS
ISO 27002	7.1.1 Inventory of assets
	7.1.2 Ownership of assets
	12.6.1 Control of technical vulnerabilities

5.4.5. Post-Change Security Verification

Post Change Security Verification is an audit control to ensure that no unexpected risks have been introduced into the infrastructure as a result of a change.

As it is often difficult to identify all functional issues and vulnerabilities prior to deployment in production, all implementation plans should include appropriate functional and security verification testing once the change has been deployed. As part of the proposed change review, the Change Manager reviews the post change functional and security verification testing identified in the implementation plan. Approval of the proposed change is dependent on assurance that post change functional and security verification tests meet the organization's requirements for ensuring availability and security of the service.

The change window should include sufficient time to execute functional and security verification testing and to back out the change if test results are unacceptable. Once the change has been implemented, the functional testing and security testing should be executed. Unacceptable results from either the functional testing or the security validation testing should trigger a back out of the change.

Not all verification testing identified for pre-change security verification may be required for post change security verification. For example, the Change Manager may determine that input and output validation testing is required as a condition of approval of a proposed change but not required for post change security validation. Post change

security verification testing is typically a subset of the security acceptance testing conducted as part of service validation and testing (see section *5.3.1 Security Acceptance Testing*) and may include penetration testing, vulnerability scans and/or port scans.

References

Standard	Section
ITIL v3	Service Transition: Service Validation and Testing: 4.5.4.10 Types of testing – Table 4.2 Examples of Service Management manageability tests
ISO 27001	4.2.2 Implement and operate the ISMS
ISO 27002	10.3.2 System acceptance
	12.2.1 Input data validation
	12.2.2 Control of internal processing
	12.2.3 Message Integrity
	12.2.4 Output data validation
	12.5.4 Information leakage

5.4.6. Change Reconciliation

Both ITIL and ISO 27002 identify the requirement to measure conformance to Change Management policies and processes. Change reconciliation is an audit control to ensure that all changes implemented in the infrastructure have been approved.

In order to ensure that all changes in the infrastructure have been approved it is necessary to reconcile actual changes implemented in the infrastructure against approved Requests for Change (RFCs).

An unauthorized change is considered by ISO 27002 to be a security incident. For this reason, Change reconciliation should be conducted, where feasible, on a daily basis (see section *Periodic Review of Security Events*). An unauthorized change could result in unacceptable risks in the infrastructure. An unauthorized change could occur as a result of personnel failing to follow change management processes or as a result of malicious activity.

Most components (operating systems, network devices, applications, etc.) in the system are capable of logging configuration change events. Configuration change log data is critical to reconciling actual changes to approved changes.

An important consideration in change reconciliation is the completeness and integrity of configuration change log data generated by devices and applications. ISO 27002 identifies the requirement to protect log data from tampering to reduce the risk that evidence of unauthorized changes is removed from the logs.

Change reconciliation is very labour intensive without a centralized log management system which can collect and store log data as well as generate reports on all logged configuration changes. Many centralized log management systems also provide mechanisms to prevent the log data from being tampered with.

Change Reconciliation requires that appropriate logging levels are configured on all components to log configuration changes and that log data is collected and retained for the duration identified in the Log Management policy.

In order to reconcile actual changes to approved changes, all configuration change records from device and application logs must be extracted and map each change to an approved request for change.

If a change cannot be reconciled to an authorized RFC then an incident ticket should be created. Incident response for all unauthorized changes may include backing out the unauthorized change as soon as possible.

References

Standard	Section
ITIL v3	Service Design: Information Security Mgmt: 4.6.6 Triggers, inputs, outputs and interfaces
	Service Transition: 4.2 Change Management
ISO 27001	4.2.3 Monitor and review the ISMS
ISO 27002	10.1.2 Change management
	10.10.3 Protection of log information
	12.5.1 Change control procedures

Author Name, email@address

5.5. Knowledge Management

5.5.1. Security Awareness Education & Training

Security awareness is a critical security control. If employees, contractors and third party users do not act in compliance with the organization's security policy then unacceptable risks may be introduced into the infrastructure.

Both ITIL and ISO 27002 identify the requirement for security awareness education and training. Security awareness education and training should be developed by the organization and conducted periodically (e.g. yearly) to ensure ongoing compliance. The security awareness education and training program should also include provision for periodically assessing security awareness levels and delivering knowledge transfer to address deficiencies in employee, contractor or third party user compliance.

The goal of security awareness education and training is to reduce the risk of a human error resulting in a security breach by ensuring that employees, contractors and third party users are aware of information security threats and concerns as well as their responsibilities and liabilities. Security awareness education and training also ensures that employees, contractors and third party users are aware of and are equipped to support the organization's security policies.

Employees, contractors and third party users should be familiar with the content of the organization's security policies and where to find them. They should understand how the policies relate to their job functions and their responsibilities for acting in compliance with security policies and all service management processes and procedures. All personnel should also understand their responsibilities for reporting instances of non-compliance, security weaknesses or potential security incidents and be familiar with the reporting procedures.

In addition personnel should be made aware of their job specific responsibilities and follow the established procedures (e.g. technical support personnel must follow the change management process, personnel involved in developing new releases must ensure that security controls are incorporated into releases, etc.).

Security education and training should also include ensuring that all personnel are aware of disciplinary actions that could be taken against them in the event of noncompliance.

The actual mechanisms to deliver security awareness education and training are dependent on the organization's specific requirements and on the learning styles of different target groups. Security awareness education and training can take the form of formal classroom training, web-based training, user guides, journals and/or newsletters.

The CAG states several specific awareness requirements including ensuring that all personnel who have access to administrative accounts use these accounts only for administration activities and ensuring that administrators use different passwords for their admin and non-admin accounts. The CAG also identifies the requirement for job specific security awareness including roles and responsibilities for various security incident scenarios.

References

Standard	Section
ITIL v3	Service Transition: 4.7 Knowledge Management
ISO 27001	5.2.2 Training, awareness and competence
ISO 27002	8.2.1 Management responsibilities
	8.2.2 Information security awareness, education, and training
	8.2.3 Disciplinary process
CAG (SANS)	Critical Control 8: Controlled User of Administrative Privileges – subcontrols 6, 7
	Critical Control 18: Incident Response Capability – subcontrol 5
	Critical Control 20: Security Skills Assessment and Appropriate Training to Fill Gaps – subcontrols 1, 2, 3

Author Name, email@address

6. Service Operation

Service Operation is concerned with managing and supporting the service as per agreed upon service levels.

6.1. Event Management

6.1.1. Event Logging

Devices and applications should be configured to log logged in order to detect problems and unauthorized activity in the infrastructure.

Log data should be protected against tampering and unauthorized access. System administrators should not have permission to erase or de-activate logs of their own activities. As this is often not feasible, log data should be forwarded in near real-time to a remote log repository. The log data repository should not be under the control of person who also is a system administer for any of the log sources (principle of separation of duties).

The default logging level for many host-based operating systems, network operating systems and applications is either minimal or logging is not active. Secure baselines should include configuration of required logging (see section *0*

Secure Baselines).

Clock synchronization across all components in the infrastructure is required in order to effectively correlate events.

Anton Chuvakin has recently posted recommendations for an updated version of the SANS Top 5 Log Reports on his blog site (Chuvakin, 2010). This is an excellent source for identifying what needs to be logged.

At minimum, the following events should be logged:

Event Type	Activity
Audit	Login attempts (success and failure)
	VPN authentication attempts
	Administrative activities
Changes	Configuration changes including application installs and updates
	User & Group changes – addition/change/deletion
	System file changes
	Changes to file access permissions
	Activation and de-activation of logging process(es) on log sources
Network Activity	Accepted/denied traffic outbound and inbound
	Source routing attempts
Malware	Activation and de-activation of protection systems (e.g. anti-virus systems)
	All anti-virus events
Faults	Warnings, errors and critical errors
	System and application crashes, shutdowns and restarts
	Backup failures

Event Type	Activity
Anomalous activity	Anomalous activity detected by intrusion detection/prevention systems

References

Standard	Section
ITIL v3	Service Operation: Event Management: 4.1.5.2 Event notification
ISO 27001	4.2.2 Implement and operate the ISMS
ISO 27002	10.10.1 Audit Logging
	10.10.2 Monitoring system use
	10.10.3 Protection of log information
	10.10.4 Administrator and operator logs
	10.10.5 Fault logging
	10.10.6 Clock synchronization
CAG (SANS)	Critical Control 5: Boundary Defense – subcontrols 3, 5
	Critical Control 6: Maintenance, Monitoring, and Analysis of Audit Logs – subcontrols 1, 4, 5, 8, 9
	Critical Control 8: Controlled Use of Administrative Privileges – subcontrols 10, 12
	Critical Control 9: Controlled Access Based on Need to Know – subcontrol 3

Author Name, email@address

6.1.2. Health and Performance Monitoring

Information Security Management and Availability Management are both concerned with the availability of services and information. As such, monitoring the health and performance of services is considered a security control.

Availability Management is concerned with defining specific monitoring requirements for the service (see section *4.3.2 Availability Monitoring*). Health and performance monitoring systems should be configured to monitor the metrics specified by Availability Management and generate an alert to the incident ticketing system when a threshold has been exceeded or a failure is detected.

Health and performance monitoring systems typically use mechanisms (such as SNMP or vendor proprietary protocols) to collect information about the health and performance of devices and applications as well as receive alerts (e.g. SNMP Traps) from the target systems.

References

Standard	Section
ITIL v3	Service Operation: Event Management: 4.1.5.2 Event notification
ISO 27001	4.2.2 Implement and operate the ISMS
ISO 27002	10.6.1 Network controls

6.1.3. Event Correlation & Alerting

Network monitoring systems can generate a significant volume of data. Also systems may generate thousands of log messages per day. Automated event correlation enables filtering of this data to identify events of significance to the organization.

Alerting goes hand in hand with event correlation. Correlation engines typically provide options for alerting when a correlated event is detected. Alerting options include logging the correlated event, forwarding the alert to a ticketing system, sending an email and executing a program or script (e.g. if a process fails then restart it).

Network monitoring systems typically include event correlation such as generating an alert when two or more events occur at the same time, or when a threshold is exceeded for a specified amount of time.

Most monitoring systems have the capability to trigger an automated action when an alert is triggered. Automated response actions include generating an alert to an incident ticketing system or executing a program or script to resolve the issue e.g. (if a process fails then restart it).

Intrusion detection systems (IDS) are effectively event correlation and alerting engines. Traffic in the network is directed through an intrusion detection/prevention probe which examines all traffic before passing it on through the network. The IDS correlates traffic patterns to known anomalous activity "signatures" such as the presence of a virus or unauthorized scanning activity. If the IDS detects anomalous activity it can generate an alert. If the system also has prevention capabilities (IPS), it can be configured to drop the anomalous traffic instead of forwarding it on after inspection.

Security Information and Event Managers (SIEMs) collect and store log data and perform event correlation to detect security events. Like network monitoring systems, SIEMs can be configured to trigger an automated action when an alert is triggered.

Network monitoring systems, intrusion detection/prevention systems and security information and event managers also have reporting capabilities to support manual event detection activities (see section *6.1.4 Periodic Review of Security Events*).

References

Standard	Section
ITIL v3	Service Operation: Event Management: 4.1.5.4 Event filtering
	Service Operation: Event Management: 4.1.5.5 Significance of events
	Service Operation: Event Management: 4.1.5.6 Event correlation
ISO 27001	4.2.2 Implement and operate the ISMS
ISO 27002	10.6.1 Network controls
CAG (SANS)	Critical Control 6: Maintenance, Monitoring, and Analysis of Audit Logs – subcontrol 3
	Critical Control 15: Data Loss Prevention – subcontrols 2, 3

Author Name, email@address

Standard	Section
	Critical Control 17: Penetration Tests and Red Team Exercises – subcontrol 4

6.1.4. Periodic Review of Security Events

Sophisticated security event correlation systems such as intrusion detection and security information and event management (SIEM) systems are capable of processing multiple security events to detect anomalous patterns and activities. These systems are capable of generating alerts to a network monitoring system. However some types of security events require human review in order to determine if a security incident occurred. For those types of events where manual review is required, correlation engines can provide correlated reports to aid in the identification of patterns and trends indicating potentially anomalous activity.

Depending on the nature of the event, a single security event does not necessarily imply a security incident. Often, many security events together indicate a single security incident. For example a high number of failed logins against a single user account would constitute a single security incident. Also an intrusion detection/prevention system (IDS/IPS) examines all packets that pass through it for patterns indicating anomalous activity. When the IDS/IPS detects a potential security incident it generates an alert. Note that most malware (virus, worm, Trojan horse, etc.) detection is based on correlation of multiple events to identify incidents.

Most security events individually do not require a response but event patterns may indicate a requirement for further investigation. A medium-sized company could have hundreds or thousands of security events per day. Most of these events can be ignored on an individual basis but could cumulatively indicate a significant security event. As such it is important to review security events and look for patterns that could indicate anomalous activity.

It is recommended that security events are reviewed on a daily basis where possible.

During the review of security events, if a security incident is detected an incident ticket should be created.

The types of security events which require periodic review include (but are not limited to) the following:

Event Type	Description
Login attempts	A failed login event is a security event but normally does not require investigation. However multiple failed login attempts against a user account could indicate an attempted "Brute Force" attack in progress. In this case some investigation would still be required to verify whether the event was actually a Brute Force attack or simply an authorized user who forgot his password. If it is determined that a Brute Force attack occurred then appropriate response actions are required. If the attack was successful (intruder was able to gain access) appropriate response actions could include disabling the user account and disconnecting the intruder, collection of forensic evidence and/or repair of any damage resulting from the intrusion. Successful login attempts should also be reviewed for unusual login patterns such as logins after hours, logins to multiple systems, etc.
Administrative activities	Unusual administrative activities could be an indicator of an attempt to compromise a system. Activities to be examined include user account creation/deletion/modification, modification of user privileges and access permissions, modification of permissions on application, directory or files and policy changes.
Access to Resources	Unusual access attempts could be an indicator of an attempt to compromise a system. Activities to be examined include failed attempts to gain additional privileges/permissions, denied access to resources (folder, file, etc.) and deviations from baseline access activity.
Configuration changes	Changes by nature are security events as every change

Event Type	Description
	potentially introduces new vulnerabilities into the environment. An unauthorized change to a device or application configuration is at minimum a non-conformance with Change Management policy ("all changes must follow the Change Management process"). Unauthorized changes could introduce unknown security vulnerabilities into the system as they have not gone through review and approval. Also mean-time-to-repair could be negatively impacted by an unauthorized change which results in a failure. In the worst case, the unauthorized change is due to malicious intent on the part an internal or external person. All changes logged by components need to be reconciled to approved change requests. Any changes which cannot be reconciled should be considered a security incident. See section *5.4.6 Change Reconciliation* for more information.
Fault Logs	Recurring low level faults are often a warning sign of a future failure. It is important to regularly review the fault log data generated by each component and identify any trends indicating a potential pending failure. For example as a disk drive degrades it may start reporting bad sectors. These messages tend to increase over time as the integrity of the disk drive degrades.

References

Standard	Section
ITIL v3	Service Operation: Event Management: 4.1.5.5 Significance of events
	Service Operation: Event Management: 4.1.5.6 Event correlation
ISO 27001	4.2.2 Implement and operate the ISMS
ISO 27002	10.4.1 Controls against malicious code

Author Name, email@address

Standard	Section
	13.1.1 Reporting information security events
	13.1..2 Reporting security weaknesses
	10.10.2 Monitoring system use
CAG (SANS)	Critical Control 6: Maintenance, Monitoring, and Analysis of Audit Logs – subcontrol 6
	Critical Control 8: Controlled Use of Administrative Privileges – subcontrol 9
	Critical Control 11: Account Monitoring and Control – subcontrols 2, 4, 8, 9

Author Name, email@address

6.2. Incident Management

6.2.1. Incident Response Procedures

Formal incident response procedures are especially important for responding to security related incidents. In addition to reducing mean time to repair, formal incident response procedures for security related incidents can reduce the potential damage to the organization resulting from an incident.

For security incidents it is critical to be able to contain or hold off an attack so that resources can focus on analysis, on determining a resolution and contacting authorities (where required). In the event of an attack, the risk of damage to the organization is extremely high from the time the security incident occurs until the incident is resolved. For this reason, it is critical that there are documented and tested response procedures for containment or holding off an attack. For example, when a virus is detected on a desktop, the first action would be to remove the desktop from the network immediately and then focus on removing the virus from the desktop.

All incidents follow the incident management process. However, depending on the nature of the incident, the response to the incident will vary. What is often referred to as "Security Incident Management" is really a set of security incident response guidelines and procedures and is part of Incident Management.

There are certain considerations which are unique to an incident classified as security related. Typically, organizations have a formal or informal security officer who must be notified when a security related incident is detected. The security officer assesses the impact on security and provides guidance on response.

Notification and escalation procedures for security related incidents need to address confidentiality considerations due to the potential sensitivity of a security related incident. For example if information about the incident is exposed there could be potential damage to the corporate reputation. Alternately, employee disciplinary action could result from the incident – privacy laws require strict confidentiality regarding personal information.

There may be a requirement for the security officer to notify senior management and provide periodic updates in the event of high severity security related incidents until the incident has been resolved.

It is important that all available forensic evidence is captured and that is handled correctly. Forensic evidence is used for internal incident review and/or if legal action results from the incident. Rules and appropriate procedures for the handling of forensic evidence are critical. If legal action results from the incident, then it is critical that the organization can prove that the forensic evidence has not been tampered with.

An incident can be determined to be a security incident at any point in detection, analysis or resolution activities. Multiple teams may be involved in analysis and resolution of a security incident depending on the nature of the incident. For example a ticket is opened reporting abnormal behavior of an application. The ticket is routed to the application support team who determine that an unauthorized change was made and that the application has been compromised. The application team reports the incident to the security office. The application and OS teams then collect forensic evidence, as required, and proceed with cleanup of the application (e.g. restore operating system and application from a known good backup). As part of the post incident review, the forensic evidence is analyzed and appropriate next steps identified. Next steps could include disciplinary action due to non-conformance to corporate change management policies and/or engaging law enforcement if malicious intent is suspected.

Some sample incident response procedures are summarized in the table below.

Incident	Response Examples	Benefits
Malware or virus detected	1. Disable the switch port(s) that the device is connected to (depending on the infrastructure it may be quicker to remotely disconnect the device before someone can physically remove it). 2. Physically remove the device ("quarantine it") 3. "cleanse" the device or restore from last known good backup 4. execute verification testing	The faster the contaminated device is quarantined, the lower the negative impact on the infrastructure.
Failed Component (active/standby configuration):	1. Manual or automated failover to backup component. 2. Verify functionality – verification testing 3. In next emergency change window, repair the failed component and failback to the primary component. 4. Verify functionality – verification testing	If procedure is documented then delays can be avoided as response personnel have the response procedures at hand and can manually fail over the component, if required, and verify functionality very efficiently. Reduce delays due to human error.
Failed server or application	1. Reboot server or application 2. Verify functionality – verification testing	The faster that functionality is restored, the lower the negative impact on the infrastructure.
Distributed Denial of Service Attack	Options: • disconnect network from the Internet • change firewall rules (if attack coming from limited locations) • block traffic at service provider	It is important to get management's direction on how to respond to certain types of security incidents such as distributed denial of service attacks in advance of an attack. Specific responses will depend on the nature of the organization's business. For example if a major part of the business depends on orders placed through their web site, the organization may not want to

Incident	Response Examples	Benefits
		disconnect from the Internet. In this case alternate responses need to be considered.
Unauthorized Change	1. Rollback configuration to last known good configuration (immediately? In next emergency change window?) 2. Verify functionality – verification testing	The objective is to minimize the time of any exposure between the time that the unauthorized change occurs and the time that the issue is resolved. It is a management decision whether the risk of exposure until the next emergency change window is greater than the costs related to the loss of service due to restoring the device to the last known good configuration.

References

Standard	Section
ITIL v3	Service Operation: Incident Management: 4.2.5.3 Incident categorization
	Service Operation: Incident Management: 4.2.5.7 Investigation and Diagnosis
	Service Operation: Incident Management: 4.2.5.8 Resolution and Recovery
ISO 27001	4.2.2 Implement and operate the ISMS
ISO 27002	10.1.1 Documented operating procedures
	13.2.1 (Management of information security incidents and improvements) Responsibilities and procedures
CAG (SANS)	Critical Control 18: Incident Response Capability – subcontrols 1, 2, 3, 4, 5

Author Name, email@address

6.3. Problem Management

6.3.1. Post Incident Review

The purpose of post incident reviews is to assess the effectiveness of detection, response, analysis and the overall management of information security incidents and identify actions to prevent the incident from reoccurring or, if reoccurrence cannot be prevented, to minimize the impact of future incidents.

Although post incident reviews (PIR) are not explicitly identified in either ITIL or ISO 27002, they are critical activities for both service assurance and information security.

The organization may determine that certain incidents require additional investigation to determine actions to either prevent the incident from occurring again or minimize the impact on the infrastructure if the incident reoccurs. Incidents that typically warrant post incident review include major incidents and incidents which have a high likelihood of reoccurring.

The audience of a post incident review includes customers and/or business units affected by the incident as well as technical support teams involved in the incident resolution. PIRs improve the relationship with the user community by demonstrating accountability to the users and to the business.

Post incident reviews report on the incident and should include the following activities:

- Services and users affected
- Time incident occurred
- Time incident was resolved
- Description of symptoms
- What was done to recover service and by who
- Post Incident Analysis
- Attempts to determine root cause of the incident
- Identify workarounds, as appropriate
- Identify preventive/corrective actions, as appropriate

The security team plays a role in post incident reviews. If an incident is security related then the security team may oversee the post incident review.

Preventive/corrective actions can include configuration changes, implementing additional monitoring, policy changes and/or procedural changes. From a security perspective, security should be considered in proposed preventive/corrective action items identified in the post incident reviews.

References

Standard	Section
ITIL v3	Service Operation: Problem Management: 4.4.5 Process activities, methods and techniques
ISO 27001	4.2.3 Monitor and review the ISMS
ISO 27002	13.2.2 Learning from information security incidents

6.3.2. Security Advisories and Vendor Patch Review

Prompt deployment of security patches and/or workarounds reduces the risk of a security incident resulting from the exploitation of a known vulnerability. Regular reviews of posted security advisories and new vendor security patches ensure that the organization responds quickly to reduce risks resulting from exploitation of published technical vulnerabilities.

Unpatched systems pose one of the top risks to the security of the organization. For most organizations, the probability is very high that a known vulnerability will be exploited resulting in a security incident (e.g. worms and viruses).

A number of security advisories are available via the Internet and/or on-line subscription. As well, vendors post security advisories and patches on their support websites and via subscription.

In order to mitigate the risks due to software vulnerabilities, periodic review of security advisories and vendor patches is strongly recommended. At minimum this

review should be conducted on a monthly basis as many vendors post security patches on a monthly basis (e.g. Microsoft).

Sometimes a vulnerability may be identified but a security patch is not yet available or the system cannot be patched right away. Depending on the system, it may take some time to test and implement the patch or there are constraints preventing the patch from being applied. For example an application may require a very specific version of a database and/or underlying operating system. When a security patch cannot be applied promptly, the organization needs to consider implementing additional protection (workaround, firewall rules, monitoring, etc.) to prevent the vulnerability from being exploited. Security advisories and vendors often identify workarounds for vulnerabilities which do not have a fix (security patch) available or where the fix cannot be applied immediately.

There are two general approaches to reviewing security advisories & vendor patches - centrally for the organization or by custodian team.

Centralized Patch Management

A centralized team monitors security advisories & vendor patches for all components in use in the infrastructure and provides information to the teams who manage the components. This approach is preferred for larger organizations as multiple teams may manage the same component type (reduces duplication of effort, enables centralized tracking, etc.). However it may not be feasible for smaller organizations. Patch management may be managed by the organization's security office or by the overall IT management team.

Distributed Patch Management

Support teams monitor security advisories & vendor patches for those components under their control. This approach may work well for smaller organizations but for larger organizations there is a risk of duplication of effort and inconsistencies across the infrastructure. Without central oversight, there is a risk that some vulnerabilities in the infrastructure are overlooked. Some components could inadvertently

be omitted from the reviews resulting in a higher risk of a security incident due to unpatched components.

References

Standard	Section
ITIL v3	Service Operation: Problem Management: 4.4.5.1 Problem detection
ISO 27001	4.2.3 Monitor and review the ISMS
ISO 27002	6.1.7 Contact with special interest groups
	10.4.1 Controls against malicious code
	12.1.1 Security requirements analysis and specification
	12.6.1 Control of technical vulnerabilities
CAG (SANS)	Critical Control 10: Continuous Vulnerability Assessment and Remediation – subcontrol 5

Author Name, email@address

6.4. Request Fulfillment Management

6.4.1. Verification of Requester's Credentials

Users submit Service Requests to request services from the service catalog or to request information about services. Before processing a service request, the requester's identity should be verified by an authoritative source or sources other than the requester. Other considerations include verifying that the requester has a legitimate business requirement for the service and has budgetary approval for the request.

Verification of requester credentials reduces the risk of loss or damage to the organization due to provision of services and/or information to unauthorized individuals.

References

Standard	Section
ITIL v3	Service Operation: Request Fulfillment: 4.3.5.3 Other approval
	Service Operation: Access Management: 4.5.5.1 Requesting access
	Service Operation: Access Management: 4.5.5.2 Verification
ISO 27001	4.2.2 Establish and operate the ISMS
ISO 27002	7.1.3 Acceptable use of assets
	11.1.1 Access control policy
	11.2.1 User registration
	11.2.2 Privilege Management
	11.4.1 Policy on the use of network services

6.5. Access Management

6.5.1. Requests for Access

Both ITIL and ISO 27002 identify the requirement for a formal procedure for granting access to information assets. All requests for access to information assets should be approved and an audit trail maintained in order to prevent unauthorized access to information assets.

The request for access procedure should include verifying the requester's identity and business justification for access to the asset(s) as well as a mechanism for formal approval of the request.

The following audit information should be maintained for each request for access:

- Requester's name
- Date of request
- Status (waiting for approval/approved/denied)
- Approver
- Approval date
- Justification for request
- Date access request fulfilled
- Person who fulfilled request

The approver of the request depends on what access is being requested. For example, requests for user access may be approved by the requester's manager or the business owner. Requests for administrative access should be approved by senior management.

References

Standard	Section
ITIL v3	Service Operation: Request Fulfillment: 4.3.5.3 Other approval
	Service Operation: Access Management: 4.5.5.1 Requesting access
	Service Operation: Access Management: 4.5.5.2 Verification
ISO 27001	4.2.2 Establish and operate the ISMS
ISO 27002	7.1.3 Acceptable use of assets
	11.1.1 Access control policy
	11.2.1 User registration
	11.2.2 Privilege Management
	11.4.1 Policy on the use of network services
CAG (SANS)	Critical Control 8: Controlled Use of Administrative Privileges – subcontrol 3

6.5.2. Revocation of Access Rights

In order to prevent unauthorized access to information assets, a formal procedure should be in place to revoke access to information assets promptly when no longer required. The procedure should include maintaining an audit trail of all access right revocations.

Revocation of access rights procedures support the principle of least privilege by ensuring that access rights and privileges are revoked when no longer required.

All requests for revocation of access rights should be approved by an authoritative source. The revocation of access rights procedure is typically triggered through Human Resources processes.

The revocation of access rights procedures should be triggered immediately when a user no longer has a business requirement for access, access rights are to be revoked as part of disciplinary action, the user is away from the office for an extended period, or when the user leaves the organization.

Revocation of access right procedures should include maintaining an audit trail identifying the user affected, the date requested, the requester, what access right were revoked, date the access rights were revoked and the person who applied the access right change.

References

Standard	Section
ITIL v3	Service Operation: Access Management: 4.5.5.2 Verification
	Service Operation: Access Management: 4.5.5.6 Removing or restricting rights
ISO 27001	4.2.2 Establish and operate the ISMS
lISO 27002	11.1.1 Access control policy
	11.2.1 User registration
	11.2.2 Privilege Management
	11.4.1 Policy on the use of network services
CAG (SANS)	Critical Control 11: Account Monitoring and Control – subcontrol 3

6.5.3. Periodic Review of Access Rights

In order to verify compliance with the organization's access control policies, actual users' access rights should be reviewed periodically.

All actual rights and privileges must correlate to approved requests for access. Any instance of non-compliance should be considered a security incident and an incident ticket created. In this case incident response would include immediate revocation of the non-compliant access rights.

The access rights review should include verification that access rights are revoked promptly when a user no longer has a business requirement for access, access rights are to be revoked as part of disciplinary action, the user is away from the office for an extended period, or when the user leaves the organization.

References

Standard	Section
ITIL v3	Service Operation: Access Management: 4.5.5.5 Logging and tracking access
ISO 27001	4.2.3 Monitor and review the ISMS
ISO 27002	11.1.1 Access control policy
	11.2.4 Review of user access rights
	11.2.2 Privilege Management
	15.2.1 Compliance with security policies and standards
	15.2.2 Technical compliance checking
CAG (SANS)	Critical Control 11: Account Monitoring and Control – subcontrols 1, 2, 6, 7

6.5.4. Periodic Review of Access Attempts

Attempts (success and failure) to access information assets should be periodically reviewed in order to minimize potential loss and/or damage resulting from unauthorized activity. Unusual access attempts could be an indicator of an attempt to compromise a system.

When anomalous activity is detected, an incident ticket should be created.

The review of access attempts should include the following activities:

Activity	Events of Interest
Access Attempts	• Failed attempts to gain additional privileges/permissions • Denied access to resource (folder, file, etc.) • Deviations from baseline access activity (e.g. increase in logins/login attempts in off hours)
Administrative Activities	• User account creation/deletion/modification • Modification of user privileges and access permissions • Modification of permissions on applications, directories or files • Policy changes

References

Standard	Section
ITIL v3	Service Operation: Access Management: 4.5.5.5 Logging and tracking access
ISO 27001	4.2.3 Monitor and review the ISMS
ISO 27002	11.1.1 Access control policy
	15.2.1 Compliance with security policies and standards
	15.2.2 Technical compliance checking
CAG (SANS)	Critical Control 11: Account Monitoring and Control – subcontrol 4, 5

Author Name, email@address

7. Continual Service Improvement

Continual Service Improvement is concerned with ensuring that the service continues to meet the organization's requirements throughout the service lifecycle.

7.1. Review Effectiveness of Processes

A periodic review of all processes ensures that they continue to be effective and efficient as the service evolves and business requirements change over time.

A key focus for periodic process reviews is examining options for improving processes. Also, processes are not effective if they are not being followed. Non-conformance to a process could be the result of deficiencies in the process or a lack of knowledge about the process.

It is important to obtain input directly from personnel who use the processes as they are in the best position to identify inefficiencies.

References

Standard	Section
ITIL v3	All ITIL v3 processes
ISO 27001	4.2.3 Monitor and review the ISMS
ISO 27002	6.1.1 Management commitment to information security
	15.2.1 Compliance with security policies and standards

7.2. Review of Security Policies

In order to ensure ongoing conformance to the organization's requirements and relevant laws and regulations, both ISO 27002 and ITIL recommend that the organization's security policies be reviewed periodically and updated as required. ITIL v3 recommends that all security policies should be reviewed at least annually but a review may also be triggered by:

- New or changed security requirements (e.g. PCI-DSS compliance)

- Security incidents which indicate gaps in the security policies
- New or changed threats and vulnerabilities
- Results from security reviews or audits

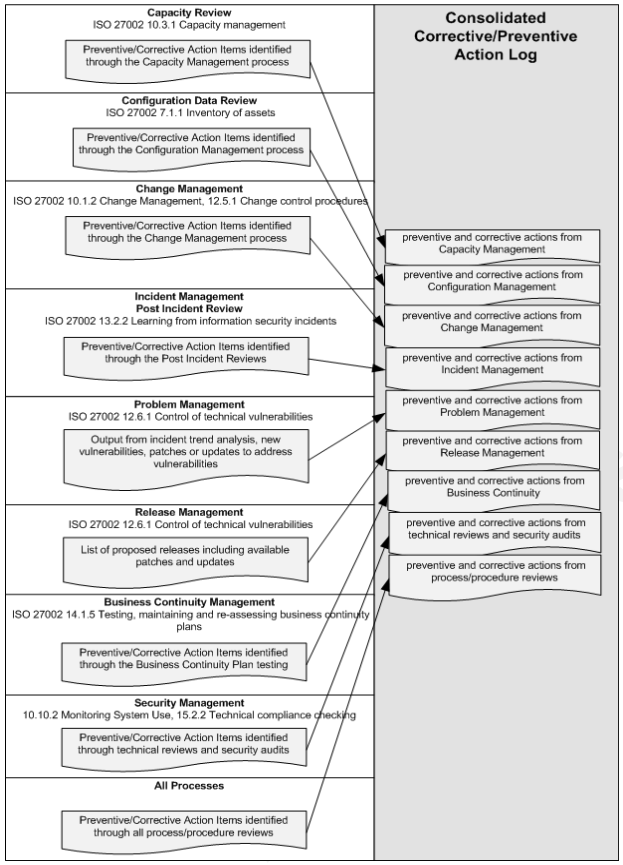
References

Standard	Section
ITIL v3	Service Design: Information Security Management: 4.6.4.2 The Information Security Policy
ISO 27001	4.2.3 Monitor and review the ISMS
ISO 27002	5.1.1 Information security policy document
	5.1.2 Review of the information security policy
	15.1.1 Identification of applicable legislation
	15.1.4 Data protection and privacy of personal information

7.3. Preventive/Corrective Actions Management

Preventive and corrective actions are identified in the course of most service assurance processes. Preventive and corrective action items are effectively repairs and improvements to be applied to the infrastructure. Typically operational teams manage their own lists of preventive and corrective actions. From both the service assurance and security perspectives there is significant value in consolidating all preventive/corrective action items (see below).

Figure 1: Flow of Process Action Items to the Consolidated Action Log



Auditors will want evidence that preventive/corrective actions are identified, prioritized, tracked and completed.

The Security Office can provide guidance to management regarding security considerations related to preventive/corrective action items. For example the Security Office can assess risks and identify security considerations related to preventive/corrective action items. The Consolidated Preventive/Corrective Actions List is a key input into technical reviews, security planning and risk assessments.

Maintaining a consolidated corrective/preventive action log enables the organization to more efficiently allocate budget & resources. In addition management has increased visibility into activities and workloads. Preventive/corrective actions identified in service assurance processes may be part of a larger project but more typically require less than three days to complete. As preventive/corrective actions tend to be a collection

of many minor tasks, management may not have a good understanding of the overall effort required to complete all of the action items. A consolidated list of all identified preventive/corrective actions associated with a system provides management with better visibility into activities and workloads. As well, this list provides insight into the current security posture of the system and is useful input into risk assessments and future security planning.

Consolidation of all preventive/corrective actions enables the alignment of preventive and corrective actions to corporate objectives and priorities. The increased management visibility into all preventive/corrective actions items enables the organization to effectively balance resource availability and budgeting against the priority and urgency of action items.

Periodic management reviews of the Consolidated Preventive/Corrective Actions List enable all service assurance teams to ensure that activities related to identified preventive/corrective action items are in alignment with overall corporate objectives and requirements. Management review of the Consolidated Preventive/Corrective Actions List provides the organization with the opportunity to step back and prioritize from an overall business perspective. Action items can be prioritized from a corporate perspective instead of by individual teams' perspectives.

Decisions on the priority of preventive/corrective action items are often made on a process by process basis often with minimal outside input. This can result in conflicts of interest - priority for one team may not be priority for another.

A consolidated action item list coming out of all processes and procedures in the service infrastructure enables the organization to effectively assess the risks and benefits of each action and determine where funding and resources need to be focused. The organization achieves this by periodically stepping back and reviewing each preventive/corrective action item and, at minimum, asking the following questions:

- What is the risk if we don't complete this right away?
- Is it feasible / possible to do this at this time?
- Is this in alignment with current or future corporate objectives?
- Do we have the funding to do this?

Author Name, email@address

- Do we have the resources to do this within the timeframes specified?
- Is there an overall cost/benefit?
- How will this affect the current security infrastructure?
- How will this affect functionality or performance of the infrastructure?

Preventive/corrective actions management provides oversight to ensure that action items are identified, tracked and completed in alignment with corporate business and security policies and objectives.

References

Standard	Section
ITIL v3	Service Design: Information Security Mgmt: 4.6.5 Process activities, methods and techniques
	Service Design: Information Security Mgmt: 4.6.6 Triggers, inputs, outputs and interfaces
ISO 27001	4.2.3 Monitor and review the ISMS
	4.2.4 Maintain and improve the ISMS
	8 ISMS improvement
ISO 27002	13.2.2 Learning from information security incidents

7.4. Non-Conformance Management

Corporate policies effectively identify how much risk the corporate can tolerate. Policies typically address, but are not restricted to, legal considerations, minimizing security risks, and budget and financial considerations. Failure to conform to the organization's policies could result in increased risks to the organization.

In order to meet ITIL and ISO 27001/2 requirements, all non-conformances to policies, standards, processes or procedures should be reported. Non-conformances may be reported by end-users, IT support and administrators, process managers or any other person who has some interaction with the system. Non-conformances to be reported include the failure of an employee or end-user to follow a process and any action or condition which is not in conformance with corporate policies.

Both ITIL and ISO 27001/2 identify monitoring, review and continuous improvement as key elements in attaining and maintaining conformance. Non-conformance report logs provide feedback on the effectiveness of policies, standards, processes and procedures. This information is essential for identifying where improvements need to be made. Auditors will want evidence that the organization has the appropriate policies in place and that there is a process in place for reporting and managing non-conformances.

It is not sufficient to have documented policies, standards, processes and procedures in place. Conformance to the organization's policies, standards, processes and procedures must also be monitored and all identified preventive or corrective action items tracked to completion.

Failure to follow a process could result in increased risks to the infrastructure. These risks include the risk of failure to meet contractual obligations, legal or regulatory requirements, and increased security vulnerabilities in the infrastructure.

Failure to follow a policy/standard/process/procedure could also indicate that some revision is required.

References

Standard	Section
ITIL v3	Service Design: Information Security Mgmt: 4.6.5 Process activities, methods and techniques
	Service Design: Information Security Mgmt: 4.6.6 Triggers, inputs, outputs and interfaces
ISO 27001	4.2.3 Monitor and review the ISMS
	4.2.4 Maintain and improve the ISMS
ISO 27002	15.2.1 Compliance with security policies and standards
	15.2.2 Technical compliance checking

Author Name, email@address

7.5. Security Risk Assessments

Periodic risk assessments enable the organization to identify risks in the infrastructure and determine appropriate mitigation required to reduce the risks to a level that is acceptable to the organization.

Security risk assessment activities include identification of acceptable risk levels, quantification and prioritization of risks and identification of required mitigation for unacceptable risk levels.

References

Standard	Section
ITIL v3	Service Design: Information Security Mgmt: 4.6.5 Process activities, methods and techniques
ISO 27001	4.2.1 Establish the ISMS
	4.2.3 Monitor and review the ISMS
ISO 27002	4.1 Assessing security risks
	4.2 Treating security risks
	9.1.1 Physical security perimeter
	10.6.2 Security of network services
	14.1.2 Business continuity and risk assessment
	15.2.2 Technical compliance checking

7.6. Technical Infrastructure Review

In order to ensure that systems maintain compliance with the organization's security policies and standards, ISO 27001 identifies the requirement for periodic technical infrastructure reviews.

Technical infrastructure review activities include vulnerability scans, port scans and penetration tests.

As business requirements change over time, it is important to periodically reassess what services and protocols are authorized for use in the organization. Port scans are useful to verify that only approved protocols and services are active. Most vulnerability scanners include port scanning functionality.

Vulnerability scans enable the organization to determine the actual vulnerabilities that exist in the network. It is recommended that, at minimum, weekly automated vulnerability scans are executed against all components in the organization's network both from the Internet and internally. Comparison of back-to-back vulnerability scans enables verification that vulnerabilities previously identified have been addressed (e.g. patches implemented, compensating controls functioning as expected, residual risks have been accepted).

Also recommended is quarterly execution of vulnerability scans in authenticated mode (scanner has appropriate access rights).

Penetration testing tools scan for vulnerabilities and then attempt to exploit each vulnerability detected using known attack vectors. Regular penetration testing from both outside and within the network is recommended. Penetration testing complements vulnerability scanning as it provides additional information about the susceptibility of existing vulnerabilities to exploitation. Penetration testing can potentially be service affecting so is typically executed less frequently than vulnerability scanning.

To ensure that personally identifiable information (PII) is not stored in clear text, periodic automated scans of servers should be executed which look for PII keywords.

Technical infrastructure review deliverables include a report which summarizes findings, identifies recommended preventive/corrective actions and identifies all detected non-conformances.

References

Standard	Section
ITIL v3	Service Design: Information Security Mgmt: 4.6.5 Process activities, methods and techniques
ISO 27001	4.2.3 Monitor and review the ISMS
ISO 27002	10.10.2 Monitoring system use
	15.2.2 Technical compliance checking
CAG (SANS)	Critical Control 5: Boundary Defense – subcontrol 8
	Critical Control 7: Application Software Security – subcontrol 3
	Critical Control 10: Continuous Vulnerability Assessment and Remediation – subcontrols 1, 2, 3, 4, 6
	Critical Control 14: Wireless Device Control – subcontrols 3, 7
	Critical Control 15: Data Loss Prevention – subcontrol 3
	Critical Control 17: Penetration Tests and Red Team Exercises – subcontrols 1, 2, 3
	Critical Control 20: Security Skills Assessment and Appropriate Training to Fill Gaps – subcontrol 3

7.7. Independent Security Review

In order to ensure effective management of security in the infrastructure, an independent review should be conducted periodically and when significant changes to the infrastructure have been implemented.

The review should be conducted by individuals who are independent of the area under review (e.g. someone from an unrelated team in the organization, internal audit team or external auditor).

An independent security review may cover the entire infrastructure or be limited to specific components. The scope of each security review is determined by management.

References

Standard	Section
ITIL v3	Service Design: Information Security Mgmt: 4.6.5 Process activities, methods and techniques
ISO 27001	4.2.3 Monitor and review the ISMS
ISO 27002	6.1.8 Independent review of information security
	15.3.1 Information systems audit controls

Author Name, email@address

8. References

Brenton, Chris, Bird Tina & Ranum, Marcus J., SANS Top 5 Essential Log Reports Version 1.0, SANS, retrieved September 28, 2010 from http://www.sans.org/security-resources/top5_logreports.pdf

Chuvakin, Anton (2010), Blog – "Security Warrior" *Updated With Community Feedback SANS Top 7 Essential Log Reports DRAFT 2,* retrieved September 28, 2010 from http://chuvakin.blogspot.com/2010/08/updated-with-community-feedback-sans_06.html

Chuvakin, Anton A. & Williams, Branden R (2010)., PCI Compliance Understand and Implement Effective PCI Data Security Standard Compliance, Syngress

International Organization for Standardization (2005), *ISO/IEC 27001 Information technology – Security techniques – Information management systems – Requirements*, ISO

International Organization for Standardization (2005), *ISO/IEC 27002 Information technology – Security techniques – Code of practice for information security management*, ISO

Office of Government Commerce (2007), *Continual Service Improvement*, The Stationary Office

Office of Government Commerce (2007), *Service Design*, The Stationary Office

Office of Government Commerce (2007), *Service Operation,* The Stationary Office

Office of Government Commerce (2007), *Service Strategy*, The Stationary Office

Office of Government Commerce (2007), *Service Transition*, The Stationary Office

PCI Security Standards Council (July 2009), *Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures Version 1.2.1*, retrieved from https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

SANS (2009), *Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines (CAG) Version 2.3*, retrieved September 28, 2010 from http://www.sans.org/critical-security-controls/guidelines.php

Author Name, email@address

Last Updated: October 23rd, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Seattle 2017	Seattle, WAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, AE	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Amsterdam 2017	Amsterdam, NL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Milan November 2017	Milan, IT	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Miami 2017	Miami, FLUS	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Paris November 2017	Paris, FR	Nov 13, 2017 - Nov 18, 2017	Live Event
Pen Test Hackfest Summit & Training 2017	Bethesda, MDUS	Nov 13, 2017 - Nov 20, 2017	Live Event
SANS Sydney 2017	Sydney, AU	Nov 13, 2017 - Nov 25, 2017	Live Event
GridEx IV 2017	Online,	Nov 15, 2017 - Nov 16, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CAUS	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, GB	Nov 27, 2017 - Dec 02, 2017	Live Event
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZUS	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Khobar 2017	Khobar, SA	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Austin Winter 2017	Austin, TXUS	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Munich December 2017	Munich, DE	Dec 04, 2017 - Dec 09, 2017	Live Event
European Security Awareness Summit & Training 2017	London, GB	Dec 04, 2017 - Dec 07, 2017	Live Event
SANS Bangalore 2017	Bangalore, IN	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Frankfurt 2017	Frankfurt, DE	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DCUS	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS SEC460: Enterprise Threat Beta	San Diego, CAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, NL	Jan 15, 2018 - Jan 20, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SEC599: Defeat Advanced Adversaries	San Francisco, CAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS San Diego 2017	OnlineCAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced