# Security Operations

- Administrative management responsibilities
- Operations department responsibilities
- Configuration management
- Trusted recovery states
- Redundancy and fault-tolerant systems
- E-mail security
- Threats to operations security

# Operations security

pertains to everything that takes place to keep networks, computer systems, applications, and environments up and running in a secure and protected manner.

It ensures the computer system function correctly by mitigating the vulnerabilities and threats to the computer operations.

**It consists of ensuring.**

- ➢ People.
- ➢ Applications.
- ➢ Servers.
- ➢ Environment.

Are properly and adequately secured and have the proper access privileges to only the resources they are entitled to and that oversight is implemented via monitoring, auditing, and reporting controls.

# The Role of the Operations Department

The continual effort to make sure the correct policies, procedures, standards, and guidelines are in place and being followed is an important piece of the **due care and due diligence efforts** that companies need to perform.

The right steps need to be taken to achieve the necessary level of security, while balancing ease of use, compliance with regulatory requirements, and cost constraints. It takes continued effort and discipline to retain the proper level of security.

operations security is the practice of continual maintenance to keep an environment running at a necessary security level, liability and legal responsibilities also exist when performing these tasks.

Companies, and senior executives at those companies, often have legal obligations to ensure that resources are protected, safety measures are in place, and security mechanisms are tested to guarantee they are actually providing the necessary level of protection.

**An organization must consider many threats.**

- ➔ Disclosure of confidential data.
- ➔ Theft of assets,
- ➔ Corruption of data,
- ➔ Interruption of services,
- ➔ Destruction of the physical or logical environment.

It is important to identify systems and operations that are sensitive (meaning they need to be protected from disclosure) and critical (meaning they must remain available at all times).

It is also important to note that while organizations have a significant portion of their operations activities tied to computing resources, they still also rely on physical resources to make things work, including paper documents and data stored on micro-film, tapes, and other removable media.

A large part of operations security includes ensuring that the physical and environmental concerns are adequately addressed, such as temperature and humidity controls, media reuse, disposal, and destruction of media containing sensitive information.

operations security is about

configuration,
performance,
fault tolerance,
security,
and accounting and verification
management

to ensure that proper standards
of operations and compliance
requirements are met.

# Administrative Management

Is a very important piece of operations security.

One aspect of administrative management is dealing with personnel issues.

**This includes separation of duties and job rotation.**

# Separation of Duties

- Is to ensure that one person acting alone cannot compromise the company's security in any way.
- no person should have too much access to a system that allows you to execute transactions in a process of business without controls and authorizations.
- High-risk activities should be broken up into different parts and distributed to different individuals or departments. That way, the company does not need to put a dangerously high level of trust in certain individuals.
- Helps prevent mistakes and minimize conflicts of interest that can take place if one person is performing a task from beginning to end.

# Un enfoque basado en riesgos para la segregación de funciones
Ernst & Young

http://www.ey.com/Publication/vwLUAssets/Perspectivas_relacionadas_con_el_riesgo_de_TI/$FILE/Enfoque_basado_en_riesgos_para_la_segregacion_de_funciones.pdf

# separation of duties

For fraud to take place, collusion would need to be committed, meaning more than one person would have to be involved in the fraudulent activity.

# separation of duties

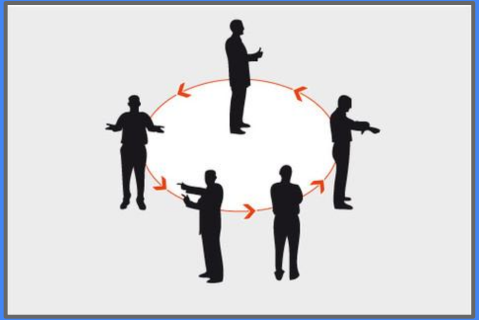
A programmer should not be the only one to test her own code. Another person with a different job and agenda should perform functionality and integrity testing on the programmer’s code, because the programmer may have a focused view of what the program is supposed to accomplish and thus may test only certain functions and input values, and only in certain environments.

| **Organizational Role** | **Core Responsibilities** |
|---|---|
| Control Group | Obtains and validates information obtained from analysts, administrators, and users and passes it on to various user groups. |
| Systems Analyst | Designs data flow of systems based on operational and user requirements. |
| Application Programmer | Develops and maintains production software. |
| Help Desk/Support | Resolves end-user and system technical or operations problems. |

| | |
|---|---|
| IT Engineer | Performs the day-to-day operational duties on systems and applications. |
| Database Administrator | Creates new database tables and manages the database. |
| Network Administrator | Installs and maintains the local area network/wide area network (LAN/WAN) environment. |
| Security Administrator | Defines, configures, and maintains the security mechanisms protecting the organization. |
| Tape Librarian | Receives, records, releases, and protects system and application files backed up on media such as tapes or disks. |

# ROLES AD DS

# Job Rotation



More than one person fulfills the tasks of one position within the company.

This enables the company to have more than one person who understands the tasks and responsibilities of a specific job title, which provides backup and redundancy if a person leaves the company or is absent

Job rotation also helps identify fraudulent activities, and therefore can be considered a detective type of control.

**Least privilege and need to know are also administrative type controls that should be implemented in an operations environment.**

**Least privilege**

means an individual should have just enough permissions and rights to fulfill his role in the company and no more.

**need to know**

Each user should have a need to know about the resources that he is allowed to access.

A system can operate in different modes depending on the sensitivity of the data being processed, the clearance level of the users, and what those users are authorized to do.

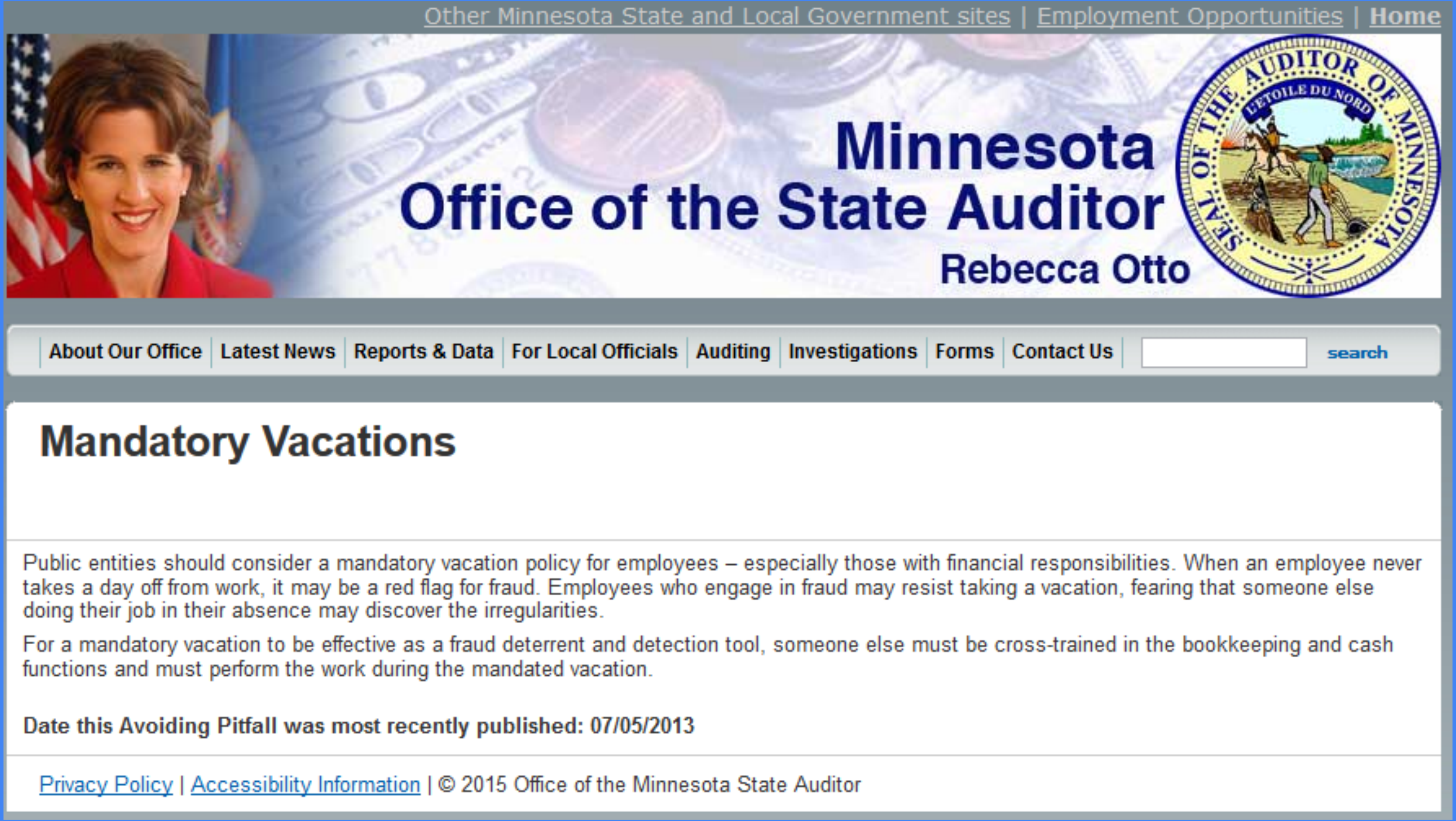
The mode of operation describes the conditions under which the system actually functions.

The goal is to reduce the incidents of fraud or embezzlement.

If an employee knows that someone else will be covering their work for a period, they also know the risk of being discovered is much higher.

EJ: salami attack

**Mandatory vacations are another type of administrative control**


Other Minnesota State and Local Government sites | Employment Opportunities | Home
Minnesota
Office of the State Auditor
Rebecca Otto
SEAL OF THE AUDITOR OF MINNESOTA
L'ETOILE DU NORD
About Our Office
Latest News
Reports & Data
For Local Officials
Auditing
Investigations
Forms
Contact Us
search

# Mandatory Vacations

Public entities should consider a mandatory vacation policy for employees – especially those with financial responsibilities. When an employee never takes a day off from work, it may be a red flag for fraud. Employees who engage in fraud may resist taking a vacation, fearing that someone else doing their job in their absence may discover the irregularities.

For a mandatory vacation to be effective as a fraud deterrent and detection tool, someone else must be cross-trained in the bookkeeping and cash functions and must perform the work during the mandated vacation.

**Date this Avoiding Pitfall was most recently published: 07/05/2013**

Privacy Policy | Accessibility Information | © 2015 Office of the Minnesota State Auditor

# Security and Network Personnel

The security administrator should not report to the network administrator, because their responsibilities have different focuses.

**The network administrator** is under pressure to ensure high availability and performance of the network and resources and to provide the users with the functionality they request.

**The security administrator** should be within a different chain of command from that of the network personnel to ensure that security is not ignored or assigned a lower priority.

**Security mechanisms commonly decrease performance in either processing or network transmission because there is more involved: content filtering, virus scanning, intrusion detection prevention, anomaly detection, and so on.**

**The following list lays out tasks that should be carried out by the security administrator, not the network administrator.**

- Carries out security assessments.
- Implements and maintains security devices and software.
- Creates and maintains user profiles and implements and maintains access control mechanisms.
- Configures and maintains security labels in mandatory access control (MAC) environments.
- Sets initial passwords for users.
- Reviews audit logs.

# Accountability

- ➔ **Users access to resources** must be limited and properly controlled to ensure that excessive privileges do not provide the opportunity to cause damage to a company and its resources.
- ➔ **Users access attempts** and activities while using a resource need to be properly monitored, audited, and logged.
- ➔ **The individual user ID** needs to be included in the audit logs to enforce individual responsibility.
- ➔ Each user should understand his responsibility when using company resources and be accountable for his actions.

# Accountability

Capturing and monitoring audit logs

- **Helps determine if a violation has actually occurred** or if system and software reconfiguration is needed to better capture only the activities that fall outside of established boundaries.

- **If user activities were not captured and reviewed**, it would be very hard to determine if users have excessive privileges or if there has been unauthorized access.

**Auditing needs to take place in a routine manner**.

If no one routinely looks at the output, there really is no reason to create logs

Audit and function logs often contain too much cryptic or mundane information to be interpreted manually.

Logs should be monitored and reviewed, through either manual or automatic methods, to uncover suspicious activity and to identify an environment that is shifting away from its original baselines.

**This is how administrators can be warned of many problems before they become too big and out of control.**

Are users accessing information and performing tasks that are not necessary for their job description?

Are repetitive mistakes being made?

Do too many users have rights and privileges to sensitive or restricted data or resources?

When monitoring, administrators need to ask certain questions that pertain to the users, their actions, and the current level of security access.

# Clipping Level

- Companies can set predefined **thresholds** for the number of certain types of errors that will be allowed before the activity is considered suspicious.
- Once this **clipping level** has been exceeded, further violations are recorded for review.
- The goal of using clipping levels, auditing, and monitoring is to discover problems before major damage occurs and, at times, to be alerted if a possible attack is underway within the network.

SNORT

OSSEC

**The security controls and mechanisms that are in place must have a degree of transparency.**

This enables the user to perform tasks and duties without having to go through extra steps because of the presence of the security controls. Transparency also does not let the user know too much about the controls, which helps prevent him from figuring out how to circumvent them. If the controls are too obvious, an attacker can figure out how to compromise them more easily.

# Assurance Levels

When products are evaluated for the level of trust and assurance they provide, many times operational assurance and life-cycle assurance are part of the evaluation process.

**Operational assurance and Life-cycle assurance**

**Operational assurance** concentrates on the product's architecture, embedded features, and functionality that enable a customer to continually obtain the necessary level of protection when using the product.

**Examples of operational assurances** examined in the evaluation process are access control mechanisms, the separation of privileged and user program code, auditing and monitoring capabilities, covert channel analysis, and trusted recovery when the product experiences unexpected circumstances.

**Vendors looking to achieve one of the higher security ratings for their products will have each of these issues evaluated and tested.**

# Assurance Levels

When products are evaluated for the level of trust and assurance they provide, many times operational assurance and life-cycle assurance are part of the evaluation process.

**Life-cycle assurance** pertains to how the product was developed and maintained.

Each stage of the product’s life cycle has standards and expectations it must fulfill before it can be deemed a highly trusted product.

**Examples of life-cycle assurance** standards are design specifications, clipping-level configurations, unit and integration testing, configuration management, and trusted distribution.

**Vendors looking to achieve one of the higher security ratings for their products will have each of these issues evaluated and tested.**

# Operational Responsibilities

Operations security encompasses safeguards and countermeasures to protect resources, information, and the hardware on which the resources and information reside.

The goal of operations security is to reduce the possibility of damage that could result from unauthorized access or disclosure by limiting the opportunities of misuse.

- **Management** is responsible for employees' behavior and responsibilities.
- **The people within the operations department** are responsible for ensuring that systems are protected and continue to run in a predictable manner.
- **The operations department** usually has the objectives of preventing recurring problems, reducing hardware and software failures to an acceptable level, and reducing the impact of incidents or disruption.

Central monitoring systems and event management solutions can help pinpoint the root cause of problems and save much time and effort in diagnosing problems.

| | |
|---|---|
| **Unscheduled Initial Program Loads** [IPL] (aka Rebooting). | Investigate computers that reboot for no reason. |
| **Asset Identification and Management** (inventory management). | **Asset management** means knowing everything hardware, firmware, operating system, language runtime environments, applications, and individual libraries in the overall environment. |
| **System Controls** | **Controls must be in place to ensure that instructions are being executed in the correct security context**. The system has mechanisms that restrict the execution of certain types of instructions so they can take place only when the operating system is in a privileged or supervisor state.<br>This would include a system startup and shutdown sequence, error handling, and restoration from a known good source. |
| **Trusted Recovery** | When an operating system or application crashes or freezes, it should not put the system in any type of insecure state. The usual reason for a system crash in the first place is that it encountered something it perceived as insecure or did not understand and decided it was safer to freeze, shutdown, or reboot than to perform the current activity. |

# Responsabilidades del equipo de operaciones

# Trusted Recovery

"Whenever something goes wrong,
I just push this little button and restart.
I wish my whole life was like that!"
GLASBERGEN
©1995 Randy Glasbergen. E-mail: glasbergen@aol.com

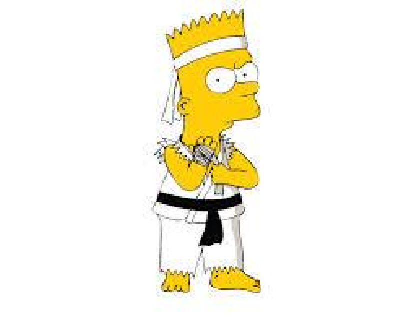
**An operating system's response to a type of failure can be classified as one of the following**

- **System reboot**
- **Emergency system restart**
- **System cold start**

| | |
|---|---|
| **System reboot** | **Takes place after the system shuts itself down in a controlled manner** in response to a kernel (trusted computing base) failure. If the system finds inconsistent object data structures or if there is not enough space in some critical tables, a system reboot may take place. This releases resources and returns the system to a more stable and safer state. |
| **Emergency system restart** | **Takes place after a system failure happens in an uncontrolled manner.** This could be a kernel or media failure caused by lower-privileged user processes attempting to access memory segments that are restricted. The system sees this as an insecure activity that it cannot properly recover from without rebooting. The kernel and user objects could be in an inconsistent state, and data could be lost or corrupted. The system thus goes into a maintenance mode and recovers from the actions taken. Then it is brought back up in a consistent and stable state. |
| **System cold start** | **Takes place when an unexpected kernel or media failure happens** and the regular recovery procedure cannot recover the system to a more consistent state. |

**It is important to ensure that the system does not enter an insecure state when it is affected by any of these types of problems, and that it shuts down and recovers properly to a secure and stable state.**

When an operating system moves into any type of unstable state, there are always concerns that the system is vulnerable in some fashion. The system needs to be able to protect itself and the sensitive data that it maintains.



# System Hardening

| | |
|---|---|
| Wiring closets should be locked. | Databases should run as a nonprivileged user, rather than as root or SYSTEM. |
| Network switches and hubs, should be inside locked cabinets. | Network ports in public places should be made physically inaccessible. |
| USB, CD-ROM or any other removable storage devices should be disabled. | Unnecessary services should be disabled or uninstalled. |
| All data on portable devices should be encrypted. | Remote Access Security. |

Even a disabled system service may include vulnerable components that an advanced attack could leverage, so it is better for unnecessary components to not exist at all in the environment.

**Locked-down systems are referred to as bastion hosts.**

**An application that is not installed, or a system service that is not enabled, cannot be attacked.**

# Remote Administration

To gain the benefits of remote access without taking on unacceptable risks, remote administration needs to take place securely. The following are just a few of the guidelines to use.

- Commands and data should not take place in cleartext (that is, they should be encrypted). For example, Secure Shell (SSH) should be used instead of Telnet.

- Truly critical systems should be administered locally instead of remotely.

- Only a small number of administrators should be able to carry out this remote functionality.

- Strong authentication should be in place for any administration activities.

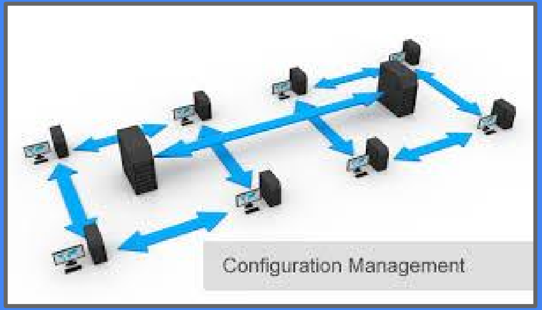
# Strong Authentication Best Practices and Use Cases

http://www.elatec-security.com/fileadmin/user_upload/ip-tv-solutions/Datasheets/Identity_Access_and_Security/Security_Solutions/Best_Practices_Final.pdf

http://www.config.fr/press/Authentication_Best_Practices_WP%28EN%29_A4_web-FINAL.pdf

http://www.gemalto.com/brochures/download/ent_Strong_Authenticaton_Best_Practices_MSFT.PDF

# Configuration Management

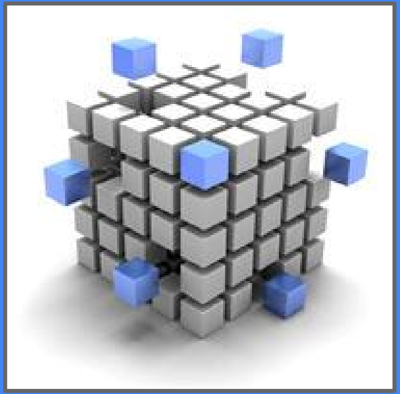


Every company should have a policy indicating how changes take place within a facility, who can make the changes, how the changes are approved, and how the changes are documented and communicated to other employees.

Without these policies in place, people can make changes that others do not know about and that have not been approved, which can result in a confusing mess at the lowest end of the impact scale, and a complete breakdown of operations at the high end.

Without strict controls and guidelines, vulnerabilities can be introduced into an environment.

# Change Control Process



A well structured change management process should be put into place to aid staff members through many different types of changes to the environment. This process should be laid out in the change control policy.

# Numerous changes can take place in a company

- New computers installed
- New applications installed
- Different configurations implemented
- Patches and updates installed
- New technologies integrated
- Policies, procedures, and standards updated

- New regulations and requirements implemented
- Network or system problems identified and fixes implemented
- Different network configuration implemented
- New networking devices integrated into the network
- Company acquired by, or merged with, another company

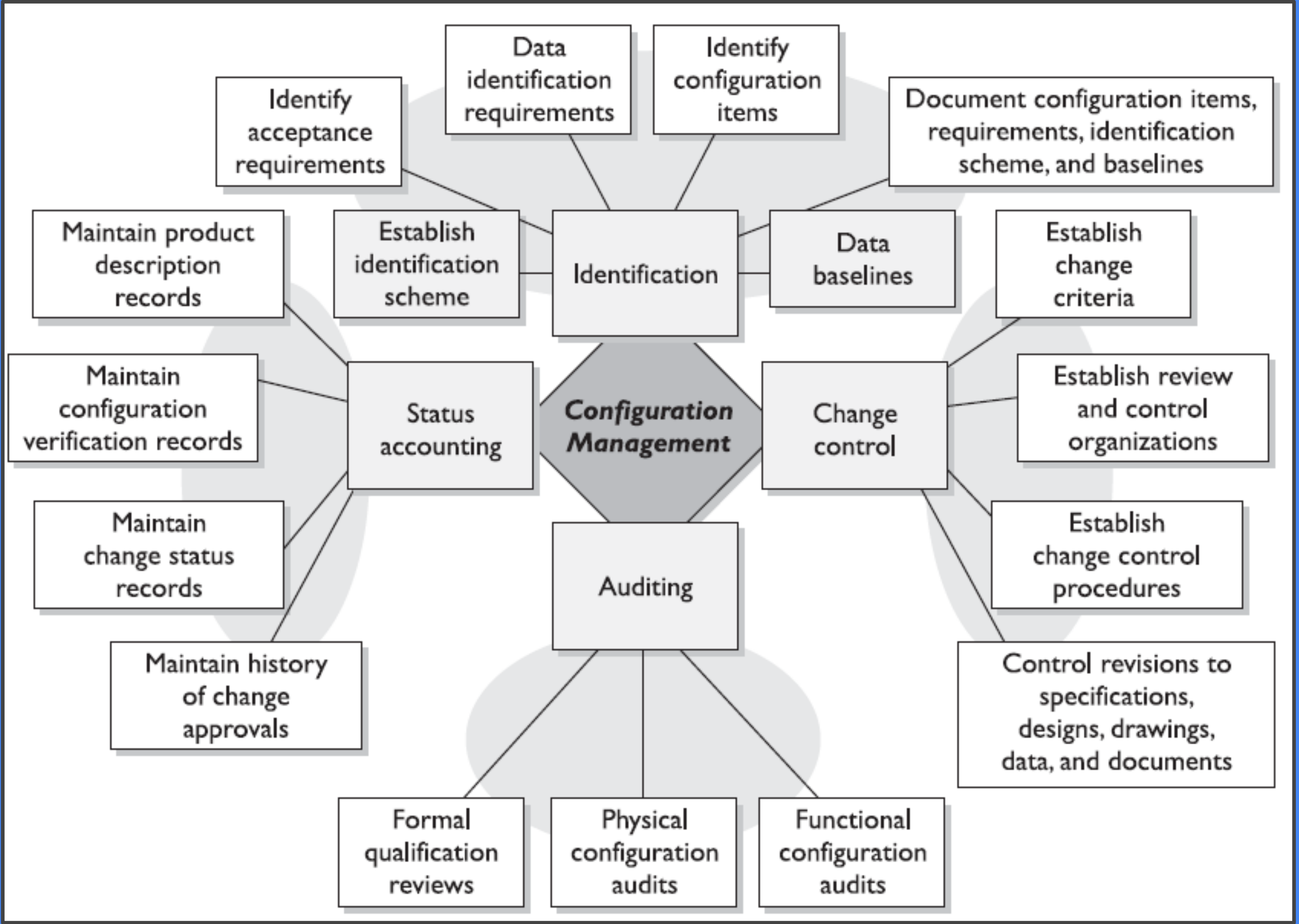
# Types of procedures that should be part of any change control policy:

| | |
|---|---|
| **Request for a change to take place** | Requests should be presented to an individual or group that is responsible for approving changes and overseeing the activities of changes that take place within an environment. |
| **Approval of the change** | The individual requesting **the change must justify the reasons and clearly show the benefits and possible pitfalls of the change.**<br>Sometimes the requester is asked to conduct more research and provide more information before the change is approved. |
| **Documentation of the change** | Once the change is approved, it should be entered into a change log. The log should be updated as the process continues toward completion. |

# Types of procedures that should be part of any change control policy:

| | |
|---|---|
| **Tested and presented** | **The change must be fully tested to uncover any unforeseen results.**<br>Depending on the severity of the change and the company's organization, the change and implementation may need to be presented to a **change control committee**. This helps show different sides to the purpose and outcome of the change and the possible ramifications. |
| **Implementation** | Once the change is fully tested and approved, **a schedule should be developed that outlines the projected phases of the change** being implemented and the necessary milestones. These steps should be fully documented and progress should be monitored. |
| **Report change to management** | A full report summarizing the change should be submitted to management. This report can be submitted on a periodic basis to keep management up-to-date and ensure continual support. |

If a server needs to have a patch applied, it is not good practice to have an engineer just apply it without properly testing it on a nonproduction server, without having the approval of the IT department manager or network administrator, and without having backup and backout plans in place in case the patch causes some negative effect on the production server.


Data identification requirements
Identify configuration items
Identify acceptance requirements
Document configuration items, requirements, identification scheme, and baselines
Maintain product description records
Establish identification scheme
Identification
Data baselines
Establish change criteria
Maintain configuration verification records
Status accounting
Configuration Management
Change control
Establish review and control organizations
Maintain change status records
Auditing
Establish change control procedures
Maintain history of change approvals
Control revisions to specifications, designs, drawings, data, and documents
Formal qualification reviews
Physical configuration audits
Functional configuration audits

# Change Control Documentation

If no one properly documents the incident and what was done to fix the issue, the company may be doomed to repeat the same scramble six months to a year down the road.

# Media Controls

Media and devices that can be found in an operations environment require a variety of controls to ensure they are properly preserved and that the integrity, confidentiality, and availability of the data held on them are not compromised.

Media should be clearly marked and logged, its integrity should be verified, and it should be properly erased of data when no longer needed.

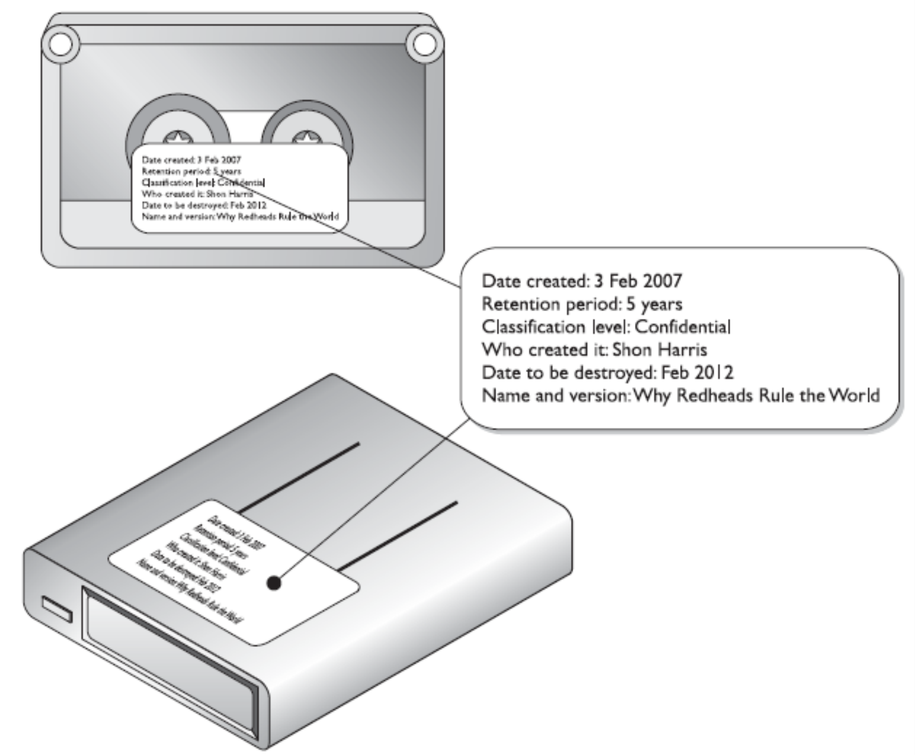
| | |
|---|---|
| **Backup tapes** | **To be properly protected from unauthorized access**.<br>they must be stored in a place where only authorized people have access to them, which could be in a locked server room or an offsite facility. |
| **Media needs to be protected from environmental issues** | such as humidity, heat, cold, fire, and natural disasters (to maintain availability), the media should be kept in a fireproof safe in a regulated environment or in an offsite facility that controls the environment so it is hospitable to data processing components. |

# Media management, whether in a library or managed by other systems or individuals, has the following attributes and tasks.

| | |
|---|---|
| **Tracking (audit logging)** | Inventorying the media on a scheduled basis |
| **Effectively implementing access controls** | Carrying out secure disposal activities. |
| **Tracking the number and location of backup versions** | Ensuring environmental conditions do not endanger media. |
| **Documenting the history of changes to media.** | Ensuring media integrity |

**Internal and external labeling**

- Date created.
- Retention period.
- Classification level.
- Who created it.
- Date to be destroyed.
- Name and version.



Date created: 3 Feb 2007
Retention period: 5 years
Classification level: Confidential
Who created it: Shon Harris
Date to be destroyed: Feb 2012
Name and version: Why Redheads Rule the World

**The media librarian responsible.**

| | |
|---|---|
| Marking | Environmental protection |
| Logging | Transmittal |
| Integrity verification | Disposal |
| Physical access protection | |

# Media Protection

# Data Leakage