Chapter 3

Controls and Safeguards

Solutions in this chapter:

- **Data Security Program**
- **Security Controls**
- **Technical Safeguards**
- **Access Control**
- **Activity Logging and Monitoring**
- **Software Assurance**
- **Change Management**
- **Disaster Recovery/Business Continuity Planning**
- **Training and Awareness**
- **Auditing**
- ☑ **Summary**

Data Security Program

An organization's data security program will enable the management and control of identified data security risks. It can significantly influence reputational, operational, legal, and strategic risks by limiting the organization's vulnerability to data compromise and maintaining third-party confidence and trust.

The data security program includes data classification and the associated risk assessment, an information security strategy to mitigate the risks, the implementation of controls to protect the data, monitoring and testing of the controls to verify that they are appropriate, effective, and performing as intended, and a process to continuously gather and analyze new threats and vulnerabilities in order to update the risk assessment, strategy, and controls.

The successful implementation of a data security program will depend on several factors, including:

- Security policies, procedures, and controls based on business objectives.
- A security approach consistent with organizational culture.
- Visible management support and commitment.
- A thorough understanding of security requirements based on a risk management approach.
- Implementation and testing of controls.
- Appropriate policy and standards distribution, training, and education.

Security Controls

Information security controls are the technical, process, physical, and policy safeguards designed to protect sensitive data by mitigating the identified and assessed risks to its confidentiality, integrity, and availability. The selection and specification of controls is accomplished as part of an organizationwide risk management and information security program and is typically dependent on risk mitigation objectives balanced by implementation cost.

Management Responsibility

Senior management has the responsibility to ensure integration of security controls throughout the organization by ensuring the security program is governed by

organizational policies and practices that are consistently applied, enforcing compliance with the security program across the organization, and ensuring an effective information security awareness program has been implemented.

In order to delineate clear lines of responsibility and accountability for information security risk management decisions, management should designate one or more individuals as information security officers, who will be responsible and accountable for administration of the security program. To ensure appropriate segregation of duties, the information security officers should report directly to the board or to senior management and have sufficient independence to perform their assigned tasks.

While information security officers may ultimately be responsible for the management of the security program and the implementation of appropriate safeguards, a system of internal control is not a separate and distinct system within an organization, but the embodiment of all the plans and devices that assure reasonable control over risks and operations. Accordingly, the responsibility for good internal controls rests with the management of the individual business units and not with any external unit. The same managers who are responsible for day-to-day operations and decision making are also responsible for ensuring the presence and effectiveness of internal controls.

Defense in Depth

Since it is practically impossible to eliminate all vulnerabilities in the organizational infrastructure, security should integrate and coordinate the capabilities of people, operations, and technology to establish multiple security countermeasures to protect the confidentiality and integrity of information assets. This multilayered defense strategy, called defense in depth (DiD), is an Information Assurance construct in which multiple related actions and controls are applied to minimize failures and compromises and their propagation.

Defense in Depth involves a multipronged and tiered approach in defense mechanisms. It is designed on the principle that multiple layers of different types of protection presenting unique obstacles will increase the likelihood of being able to identify and prevent an attack from occurring. Each protection layer has unique characteristics, presenting successive obstacles for an intruder to overcome. This will not only reduce the risk of security breaches, but allow an organization time to detect and respond to an attack, therefore reducing and mitigating the breach's impact.

Achieving Information Assurance through DiD requires a focus on three primary elements:

- **People** This includes senior level management attention, assignment of specific roles and responsibilities, commitment of resources, training of critical personnel, and personal accountability.
- **Technology** Multiple and layered technological defenses outside, at, and within the perimeter, including encryption, firewalls, intrusion detection, transmission and remote access controls, and antivirus and patch management.
- **Operations** The activities required to sustain an organization's security posture on a day-to-day basis, including security policies, risk assessments, security and vulnerability reviews, process controls, and incident response planning.

Control Identification

The challenge for organizations is to determine the appropriate set of security controls, which if implemented and determined to be effective in their application, would comply with the stated security requirements by mitigating the impact or likelihood of each identified threat. For each security category, a variety of controls are necessary for a comprehensive and robust security framework.

The following considerations should be addressed during control selection and implementation:

- What are the necessary controls to adequately protect organizational information?
- Have the selected security controls been implemented or is there a realistic plan for their implementation?
- What is the required level of assurance that the selected controls are effective as implemented?

The major factor that will influence the selection of safeguards and controls is a risk-based cost/benefit analysis. Other factors include ease of use, transparency to users, compatibility with existing controls, and integration with overall security management tools.

Control identification is accomplished most effectively as an organizationwide exercise, which considers the protection requirements for the various classes of

information. This is especially relevant since many controls may depend on other controls and processes for proper functioning.

Control identification and implementation is performed generally by a specialized team under the direction of the Information Security Office. However data owners are ultimately responsible for the proper functioning of security controls affecting their data.

Types of Controls

Controls can be categorized by what they are and what they do. The following three broad categories define the main objectives of effective security implementation:

- **Physical Controls** Security measures, devices, and means to control physical access to a defined structure.
- **Technical Controls** Technology-based measures to control logical access to sensitive information.
- **Administrative** or **Process Controls** Policies, procedures, and processes to define and guide user actions and restrictions in dealing with sensitive information.

Within these major categories, controls can be defined by what they do, including:

- **Preventive** Preventive controls act to limit the likelihood of a threat by preventing intentional or unintentional unauthorized disclosure of sensitive information.
- **Detective** Detective controls detect and report actual or attempted unauthorized events by helping identify harmful actions as they occur.
- **Corrective** Corrective controls respond to security incidents and terminate harmful events or reduce their damage.

Baseline Approach

A baseline approach to control implementation requires the establishment of a minimum set of information safeguards against the most common threats. An appropriate and justifiable baseline can be developed based on industry practice or public standards, and existing safeguards can be compared with the baseline. A gap analysis will identify applicable controls that need to be implemented.

The benefit of the baseline approach is a simplified risk assessment. However there are several risks in using this approach, including:

- The baseline does not identify all the organization's assets or accurately reflect its environment.
- Nonstandard threats or vulnerabilities are missed by the baseline.
- The gap analysis does not accurately reflect the variation between existing and required controls.
- The baseline is used as a simple checklist and acts as a substitute for all risk management.
- The baseline may be excessive for the security risk exposure as a whole or as related to a particular control.

As a result, a baseline should not be adopted without ensuring that it is appropriate to the organization's risk profile and circumstances. However, it can be useful in identifying information security strengths and weaknesses, since the result of a security baseline analysis can enable the organization to evaluate its information security posture and identify areas for improvement.

Constraints

Several constraints may arise during control implementation and may need to be resolved on a control-by-control basis. These include:

- **Time** The acceptable implementation time period based on asset sensitivity, criticality, vulnerability, and risk exposure criteria.
- **Financial** Because of conflicting demands on financial resources, a proposed control may be partially implemented and management is prepared to accept the residual risk until additional funds become available.
- **Technical** Technical and compatibility constraints can hinder the effective implementation of controls to an existing systems or data.
- **Cultural** Individual resistance to particular controls may render them ineffective, especially if staff feels that the control hinders their work and as a result develop workarounds.
- **Legal** Legal and contractual factors may mandate or bar the selection and implementation of a particular control.

- **Skills and Training** Some controls may not operate correctly if people with the necessary skills, competencies, and training are not available.

Laptops

Lost or stolen laptops represent a significant source of data compromise and are the most frequently reported information security incidents. Any sensitive data stored on a lost or stolen laptop and potentially compromised will most likely have a much greater value than the replacement cost of the actual laptop.

As a general rule, sensitive data should not be stored on laptops or any devices that can leave a secure environment. If there is a legitimate business need to store such data on a laptop, access or downloads should be logged at the source so that there is a record of what information was copied, to where, when, and by whom.

The security requirements implemented on laptops that may potentially store sensitive information should be comparable to network-based security. These include:

- Full-disk encryption to prevent unauthorized parties from retrieving the data or from extracting domain-based credentials and user account profiles that allow access to organizational network resources. Encryption passwords should adhere to complexity standards to minimize cracking risk. The organization should consider implementing systemic disk encryption solutions that do not rely on employees' discretion as to what data to encrypt.
- Any technology that can restrict usage of the laptop to a designated individual.
- Remote tracking and data reset features that once activated will ensure that files are not readable or recoverable.
- Frequent connection to the corporate network to receive the latest software patches, antivirus files, and firewall patterns.
- A prohibition on altering system software or hardware configuration unless specifically instructed to do so by IT Services.
- A prohibition on loading additional application software onto the laptop unless specifically approved by IT Services.
- Scheduled backups of all important information on the laptop.
- Implementation and adherence to a policy describing the risks of laptop loss as well as the responsibility of the user.

- An implemented policy for specifically authorizing certain laptops to process sensitive information.
- Procedures for appropriate physical securing, proper and inconspicuous packing during transportation, and general alertness to minimize risk of theft and loss.

Sufficient attention should be given to property management. This includes conducting periodic inventories of accountable property, ensuring that departing employees return all property that had been issued to them, and adequately documenting the destruction of outdated, damaged, or excessed laptops, including sanitization of all sensitive information prior to disposal.

Portable Storage Devices

Portable storage devices such as flash drives present particular challenges because their small size increases the possibility of physical loss with the attendant data loss. Additionally, the size combined with the ease of use can allow malicious insiders to inconspicuously copy large amounts of data.

Particular care should be paid to these devices since they can also impact data and network security through the intentional or unintentional bypass of perimeter defenses such as firewalls and antivirus software and introduce viruses and malware into the network.

The organization should outline in its acceptable use policy guidelines on using portable storage devices by specifying the parameters within which they can be used. Sensitive data should not be stored on a portable storage device unless the appropriate procedure is implemented and followed for obtaining management authorization for the placement of sensitive data on the device. This can be enforced through automated means that can detect when such a device is connected to an organizational resource.

If the use of these devices is allowed by the organization, data owners will have the primary responsibility authorizing the use and storage of sensitive data on them. Controls will include:

- Provisions for training to increase awareness of the need for security in this area.
- Limiting access to authorized devices or users.
- Blocking communication with specific information resources.

- Disabling file- and print-sharing functions.
- As in the case of laptops, encryption to protect any sensitive data on the device.
- Passwords that conform to the requirements and guidelines of organizational password policies.
- A prohibition on transferring sensitive data to another device not in compliance with the policy.
- Inventory and audit trail of the sensitive data used by specific individuals on specific portable devices.
- Ensuring that there is a backup of data within a secured storage environment.
- Labeling all portable devices for individual identification, such as an asset or property tag or banner containing appropriate contact information and instructions on how to return the portable device.
- Ensuring that any loss, theft, or unauthorized access is reported promptly and appropriately.

Transportable Media

Numerous business processes may require the transfer of information via transportable media such as backup tapes. The organization should evaluate all transfers of physical media containing sensitive information to discontinue unnecessary or redundant transfers either through the elimination of the transfer or through migration to network-based transmission. This determination can be made by considering the potential risk represented by the transfer, the size of the transfer, the related business process, any infrastructure limitations, legal, regulatory, or counterparty constraints, and associated costs.

If the organization determines that these transfers cannot be terminated or transmitted in-network and that physical transfers are necessary, the following controls should be implemented:

- Sensitive data in transport should be encrypted using approved encryption algorithms where feasible.
- An exact copy of the data should be maintained in case of loss or damage.

- A complete record of transport should be maintained including contents, origin and destination, time shipped and received, who handled it during transport, and condition upon arrival.
- A Risk Acceptance should be filed when the transfer is noncompliant or encryption is not possible due to regulatory issues or other reasons.

A primary compensating control for the transfer of unencrypted physical media containing sensitive information is the use of an approved secure courier service. The media must be properly packaged in a tamper-evident container and all transfer pickups and deliveries should be logged and documented, including volume serial number, tracking number, pickup or delivery time and date, as well as the name and contact information of the individual who transported the package(s).

Under certain circumstances, and where deemed appropriate and prudent, a staff member may transport unencrypted media containing sensitive information. The media must be properly packaged, the staff member must maintain physical control over the media at all times, and must obtain written acknowledgement of receipt from the recipient.

E-mail

Now we'll discuss internal and external controls for securing e-mail communications.

Internal Controls

Any electronic communications containing sensitive information should be encrypted any time it is sent outside the organization. In addition, particularly sensitive communications should be encrypted at all times, even when sent internally. Staff members should be aware of the secure e-mail encryption requirements, have an approved encryption solution installed on their desktops, and be aware of how and when to use it. In certain instances, automated and policy-driven encryption can be used to protect the confidentiality and integrity of sensitive data when in transit without the sender's intervention.

More generally, an e-mail acceptable use policy should be implemented to clearly describe applicable restrictions on the transmission of sensitive information via e-mail.

Since it relies on open ports, a particular risk of e-mail is that it allows malicious outsiders to circumvent perimeter defenses such as firewalls through the e-mail architecture. E-mail-born viruses and malware can compromise sensitive data with the added risk of spreading to partners, vendors, and competitors.

E-mail security solutions can be installed at the network boundary or at the mail server layer to filter mail based on preconfigured or configurable standards. These include content filtering for inbound mail, traffic monitoring, and reporting. Additionally, solutions can be deployed to monitor outbound e-mail to detect information patterns and restrict the transmission of sensitive information from users not specifically authorized to transmit it.

External Controls

E-mail and Internet-related fraudulent schemes present a substantial risk to the reputation and customers of any organization that is impersonated. Current and potential customers may mistakenly perceive that weak information security resulted in security breaches that allowed access to confidential information. In addition, customers who fall prey to fraudulent schemes face a real and immediate risk from malicious parties who will normally act quickly to gain unauthorized access and commit identity theft.

If warranted, an organization should consider enhancing security programs to address possible e-mail fraudulent schemes. This may include periodic notification to alert customers of known e-mail-related fraudulent schemes and to remind them to report any such requests, monitoring accounts individually or in aggregate for unusual activity, and in general avoiding sending any e-mails that request confidential information.

Technical Safeguards

In this section, we'll discuss various technical safeguards for securing systems within an organization's environment.

Firewalls

A firewall is a system, device, or collection of components configured to manage and regulate data flow between networks of different trust levels by permitting, denying, or proxying data. Although firewalls usually are placed between an internal network and an external untrusted network such as the Internet, they can also be used to create different subnets of the organizational network.

Typically, firewalls block or allow traffic based on static or dynamic rules. Static rules are preconfigured, while dynamic rules can be the result of automated coordination between the firewall and an intrusion detection system.

For a higher security environment, a possible firewall implementation is a DMZ, which is a neutral accessible zone separated by a firewall between it and the

organization's private network and another firewall between it and any external access point or network. By putting all publicly accessible services on the DMZ, which constitutes a separate logical security domain, and allowing external parties to initiate connections to services on the DMZ only, the organization can ensure that its data and systems are not directly accessible from any external source.

A firewall policy will establish the organization's expectations for how the firewall should function and stems from an ongoing security risk assessment process. It establishes a formal process for approving and testing all external network connections, as well as rules for incoming and outgoing traffic, continuing management, and changes to the firewall configuration. These rules will cover:

- Firewall types, topology, and architecture.
- Functional requirements, including access controls, baseline configurations, rules and filters, services, content restrictions, and security and authentication details.
- List of services and ports necessary for business.
- Permissible traffic, including protocols, data, and applications permitted.
- Management and maintenance, including configuration auditing and testing.
- Traffic monitoring.
- Justification and documentation for any risky protocols allowed, including reason for use of protocol and security features implemented.
- Procedures for addressing requests to bypass firewall security for specific protocols or services required for business purposes.

A review of firewall logs can alert administrators to changes to firewall policy, addition or promotion of administrative accounts, and network activity, including permitted and denied connections.

Intrusion Detection and Prevention Systems

Intrusion detection and prevention systems (IDS) are access control mechanisms that allow or disallow access based on a data traffic analysis. They monitor the events occurring in a system or network, analyze them for signs of possible incidents involving unauthorized access or actual or imminent threats of policy violation, log and report incident activity, and attempt to stop the intrusion or mitigate the effects of

the detected issue. This is done either directly or by reconfiguring a firewall or making other changes to the security environment. The organization should ensure that:

- Intrusion detection systems are placed at any location where traffic from external entities is allowed to enter controlled or private networks
- Host-based intrusion detection is placed on all sensitive systems even if they do not allow external access.
- Administrators regularly analyze logs.
- Intrusion detection signatures are frequently updated.

IDS logs can record activities such as access to privileged accounts, unusual outbound connectivity, as well as administrative access to the IDS system.

Penetration Testing and Vulnerability Scanning

Penetration testing is used to evaluate the security of a system, network, or database by simulating an attack by a malicious user. It can help determine potential vulnerabilities that may result from improper configuration, technical flaws, or operational and process weaknesses. Once security issues are uncovered, their impact is assessed and a remediation plan is developed.

The test plan should detail the scope and procedure of the test in the context of assessed threats to organizational data. Depending on the test objective, resulting action may include:

- A detailed technical report on data and system vulnerabilities.
- The outcome of the test in business risk terms.
- Short-term and tactical recommendations.
- Long-term and strategic recommendations.
- A data security improvement action plan.

The frequency of testing should be determined on the basis of risk analysis and when significant changes are implemented.

Unlike the more manual approach of a penetration test, vulnerability scanning uses automated host or network-based tools to help assess security weaknesses and risks. The tools can be run on a scheduled or ad-hoc basis and will generate a report identifying each discovered vulnerability and potential risk.

Data Transmission

Sensitive data transmission, whether through FTP, system to system, or web form submission, should be performed only over a trusted path or medium with controls to provide confidentiality, integrity, and authenticity of content. All connections from an internal system or database to other systems outside the accreditation boundary should be authorized only through the use of system connection agreements, and the connection should be monitored and controlled on an ongoing basis.

Strong cryptography and security protocols should be used to safeguard the data during transmission over open, public networks. The transfer of personal information from external parties to the organization, usually through a web site, should be accomplished via secure servers using high-level encryption.

The risks from wireless networks should be evaluated carefully and appropriate controls implemented. Default network names and administrator passwords should be changed before activating the network. Address filtering can specify which physical computer addresses can connect to the network.

Wireless network transmitting sensitive data should be security enabled and transmissions should be encrypted using protected access. Additionally, strong authentication and configuration controls should be implemented at the access point and on all clients, and unauthorized access points and clients should be monitored.

Remote Access

Remote access is any access to an organizational information resource by a user or system communicating through an external, nonorganization-controlled network or connection. The organization may deem it necessary to provide remote access to data and systems for remote workers or to support operations at remote locations. In some cases, remote access is required periodically by vendors to make regular or emergency system support.

Because of the increased risks associated with access from outside the trusted perimeter, the organization should implement policies and processes governing the conditions under which remote access is granted and terminated. Remote access should be granted based on authorized business needs, limited to the minimum privileges needed, and require management approval, with all approvals periodically reviewed and justified.

Any system remotely logging into an organizational network should have adequate antivirus and firewall protections, have all the mandated security and

configurations settings, and be properly patched. As a general practice, only devices that have been configured by organization or vendor devices that meet these requirements should be authorized to connect to the internal network.

All communications between remote users and organizational networks should be through a virtual private network (VPN), which can provide a secure communications channel across a public network. Appropriate VPN security includes:

- Encryption of all transmitted data.
- Multifactor authentication requiring factors beyond general usernames and passwords to gain access.
- Strong password and account policies.
- Automatic session time-out after a certain period of inactivity and disconnection after a certain number of incorrect logon attempts.
- Logging and analysis of remote communications.

In cases where a vendor may require remote access to a system or data for maintenance or diagnostic purposes, the vendor must implement a level of security at least as high as that implemented on the data or system being serviced, unless the component being accessed is removed from the overall system and sanitized with regard to sensitive information and also tested for potentially malicious or erroneous updates before being reconnected to the system.

External System Connections

The organization may need to provide access to and from external information systems that are outside the accreditation boundary and for which there is no direct assurance over the application of security controls or the assessment of their effectiveness. In such circumstances, the organization should verify the employment of necessary security controls on the external system or have approved connection or processing agreements with the entity hosting the external system.

Interconnection security agreements are established between the organizations that own and operate the connected systems to specify the connection requirements and describe the security controls that will be used to protect the systems and data. These controls will be adhered to by both parties and will be based on risk and data sensitivity.

Additional considerations for interconnected systems include an effective change management process to coordinate planned system changes that could affect the

interconnection and prompt notification by both sides of security incidents and system disruptions in order to facilitate a coordinated response.

Antivirus and Patches

All servers and workstations should be configured with antivirus software, which should be automatically updated from the vendor's site at least daily. In addition to persistent protection, the antivirus software should perform a complete system scan on a scheduled basis. Individual workstations should not be able to disable local antivirus software or updates.

The organization should implement procedures for handling virus infections that cannot be automatically cleaned. Such procedures can include isolating the affected device, manually attempting to remove the virus, or complete reinstallation or reconfiguration.

Centralized configuration files and identical group policies should be used to configure all workstations to an appropriately high level of security. In addition to decreasing the risk of a virus infection, this practice will also simplify general support.

Since viruses and intruders can exploit existing operating system vulnerabilities, it is important to configure all operating software to automatically receive the latest upgrades and patches. In addition, a system should be in place to scan all devices for missing patches and automatically initiates patch remediation without administrator involvement.

Isolation and Minimization

By restricting host systems to enterprise applications and operating system components, and isolating individual services to separate hosts, a potential compromise can be limited to the individual system or service and the impact on other critical services would be limited.

As part of a defense-in-depth protection strategy, the organization considers partitioning sensitive data or systems into separate domains or environments. Any connections should occur through managed interfaces consisting of appropriate boundary protection devices arranged in an effective architecture.

More generally, communities of services, systems, data, and users that operate in different security roles or zones should be isolated in separate but interconnected groups, with monitoring and controls at the external boundary and at key internal boundaries.

In the system configuration context, the principle of minimization essentially states that all software, services, protocols, or other functionality that is not required by

the system or not necessary to perform a particular function should either be disabled or not installed to eliminate the possibility of compromise. In addition to increased security, this best practice can also improve performance and simplify administration.

Access Control

Access to data should be controlled through a process that ensures that user access rights reflect defined and documented business needs and job requirements. All users must be uniquely identifiable, job requirements should be attached to user identities, access privileges for each system and data group should be identified, and access rights must be in line with defined and documented business needs and should reflect the concepts of least privilege and segregation of duties.

Access Provisioning

Organizations should have an effective process for identifying new users and recording, approving, and administering access rights. New access requests will be submitted by user management to the data or system owner for approval and processing. In certain cases, the assignment of rights may be established by the employee's role or group membership, and managed by preestablished authorizations for that group. Vendors or contractors may be granted access based on their relationship with the organization.

The data owner will review and evaluate the request based on job function, data sensitivity, least privilege, and segregation of duties. Once approved, access will be configured by the data custodians or system administrators, who should not also be end users of the system in question.

The provisioning process should include an efficient mechanism for notifying the granting authority when a user's status or role changes. This, along with system changes, will prompt a review and update of access rights. In addition, upon user leave or termination, access control privileges should be revoked in a timely manner.

In addition to normal operations, the assignment of authentication and authorization credentials should include business continuity planning responsibilities.

Authentication

Authentication is the verification of identity by a system or database based on the presentation of unique credentials to that system. Authentication contributes to the

confidentiality of data and the accountability of actions performed on systems by verifying the unique identity of a user.

Passwords are a primary method used to control access to resources and are the most common authentication mechanism. Other mechanisms include token mechanisms and biometrics. Authentication that relies on more than one credential is called multifactor authentication and is generally stronger than any single-factor methods. To determine the need for this approach, the organization should perform a risk assessment of the particular access need. If the risk assessment indicates that the use of single-factor authentication may be inadequate, it should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate risk.

At a minimum, any access to sensitive organizational assets should require a unique account with an associated password. Passwords assigned to user accounts that access sensitive data should adhere to certain password management best practices, including:

- Adhering to complexity requirements such as minimum length, avoidance of common words or terms, avoidance of personal or factual information, and inclusion of various types of characters.
- Changing the initial administrator-issued password on new accounts before first use.
- Aging implementation, which requires password changes at set intervals commensurate with the risk level of the account.
- Avoiding use of the same account and password for multiple applications or purposes.
- Avoiding sharing, writing down, or electronic storage of passwords.
- Prohibiting password reuse for a specified number of generations.
- Ability for an administrator to change or reset a user password at any time.
- Clear guidance for handling lost and compromised passwords.

Accounts should be automatically logged off after a predetermined period of inactivity and locked out due to extended lack of use. They should also be locked out due to repeated unsuccessful logon attempts. These automatic lockouts are usually temporary and automatically released after a predetermined time period. To increase security against unauthorized logon attempts, the authentication error feedback

should not specify the particular component in error, but rather return a general error message.

Any password system must balance the password strength with the user's ability to remember and maintain a stronger password and more secure password. When the balancing produces a password that is not sufficiently strong, a different authentication mechanism should be considered.

All account, password, and other user authentication information should be protected from unauthorized access or modification. An end user account should not provide access to components other than the application front-end in order to prevent the bypassing security and sign-on controls. Conversely, administrative accounts should not be used to perform end user functions. All files containing passwords or other authenticators must be encrypted and the passwords must not be transmitted in clear text.

Entitlement Reviews

An entitlement review is a periodic assessment of actual entitlement privileges and permissions to systems and data to ensure that access to particular information assets is proper and limited to the needs of the assigned role or job function as dictated by the user's manager. It allows the determination of which users have access to which systems and information, and whether that access complies with the organization's security policies. The review should examine the levels of access each individual has, conformity with the concept of least privilege, whether all accounts are still active, and whether management authorizations are current.

Entitlement reviews should be performed on a scheduled basis, with the review frequency determined by the information risk assessment. In addition, an entitlement review should be performed whenever there is a change in user status, including transfer or reassignment to another business unit, change of job responsibilities within the same business unit, leave of absence or disability leave, conversion from nonemployee to employee, and employment termination. For particularly sensitive databases or resources, the review process should be automated to report changes in permissions to the appropriate manager.

Each business unit should implement a documented process to review and verify user entitlements on a scheduled basis. An individual or group who does not perform the actual reviews should be assigned to oversee the entitlement review process. This individual or group, usually from security or compliance, will have the following responsibilities:

- Ensuring that business managers do not review their own access.
- Confirming that transferred and terminated employee entitlements were appropriately changed or revoked.
- Ensuring accurate and appropriate entitlements.
- Escalating overdue reviews and exceptions.
- Coordinating any process improvements based on issues that arise during the entitlement review process.

Privileged Accounts

Privileged accounts are functional IDs used for system administration and operation. These accounts have very few security restrictions, so they can allow a user to make unauthorized changes or to gain access to sensitive data, whether inadvertently or by design. In addition, as they are usually associated with a group or role and not directly attributable to an individual, there can be limited, if any, accountability.

Since privileged accounts are critical to operating system and application availability, and are sometimes the only IDs allowed to perform certain functions, it is usually not possible to disable or delete them. It is therefore important to manage the risks associated with them by defining their appropriate use, ownership, and control.

Account Ownership

Each privileged account should be assigned to an owner who will be able to assign the account to an administrator but who will remain responsible for all activities performed with the account. For a system processing sensitive data, the owner will be the data or application owner, who will be able to assign the account to the administrator or DBA supporting the application or database.

Upon an account owner's termination or transfer, the account should be transferred to a new owner, who will perform an entitlement review to ensure that all accounts are assigned properly.

Account Assignment and Usage

An account owner can authorize the use of a privileged account by a staff member based on:

- **Justification** The reason access is required.
- **Risk Profile** The system criticality multiplied by the account access level.

- **Least Privilege** The minimum privilege required to fulfill the person's job function.
- **Segregation of Duties** Separation of certain areas of responsibility to reduce the opportunity for unauthorized modifications or misuse.

Based on these criteria, the account owner will determine the level of access associated with the account. For particularly sensitive accounts, multifactor authentication such as smart cards or the simultaneous logon by two users should be required.

A detailed record should be kept of what privileges have been given to whom, when, and for what purpose.

Managing Account Passwords

Privileged account passwords must be changed at scheduled intervals commensurate with the risk level of the account as well as when the account owner or any authorized user leaves the organization or changes job responsibilities.

Password management best practices also require that passwords have a certain minimum length and adhere to complexity rules. In addition, password aging, inactivity threshold, and unsuccessful password attempt lockout should be implemented.

Activity Logging and Monitoring

For general security purposes and in order to demonstrate compliance to regulatory and data privacy requirements, it is essential to log and monitor all activity performed with privileged accounts. The audit log should record the user ID, log on and log off times, and activity of every session.

These activity logs should be reviewed by the account owner on a regular basis, with special attention being paid to the use of these accounts to create new user accounts or to elevate the privileges of other accounts.

Policies and Procedures

Clear policies and procedures must be in place to manage and control administrative access. They should include the following:

- **Separate User and Administrator Accounts** Users who are also administrators should have a regular account for typical end user tasks and a separate account for administrative tasks only. The passwords for these two accounts should not be the same.

- **Use Privileged Accounts Only for Relevant Tasks** The signing on to an application or database with a privileged account to perform tasks that do not directly require it should be prohibited. This will reduce security risks and prevent malicious software from running with the same privileges as the administrator.
- **Rename the Default Administrator Account** This will remove the obvious indication that this account has elevated privileges.
- **Create a Decoy Administrator Account** To add an additional layer of protection and keep any would be hackers busy, a new account named Administrator with no special privileges should be created. Its usage should be monitored for unexpected activity such as logon failures.
- **Minimize the Number of Privileged Accounts** The number of privileged accounts should be kept to an absolute minimum. This will increase control and security and reduce the administrative burden.
- **Periodically Expire Privileged Accounts** Expiration dates should be placed upon administrative accounts and they should be periodically expired to eliminate unused accounts.
- **Closely Manage Vendor Software Default Passwords** Sometimes the privileged account is the default account delivered in vendor software. These accounts present a particular risk as they are widely known and are usually the first ones that an unauthorized user will try. If possible, these accounts should be removed or obscured. Additionally, the default passwords for these accounts should be immediately changed when the software is installed.

Developer Access to Production

There are certain circumstances under which developers need access to production data or systems in order to debug a particular feature in a live system or to use realistic production data for test purposes. Since developers do not usually have the same access privileges as business users of the data and can present a particular risk because of their in-depth technical knowledge of a system, a program should be implemented to order to strengthen controls over their access to controlled information systems and to sensitive production data in nonproduction environments.

Where sensitive data is stored or used in testing or other nonproduction environments, such data must be protected using controls comparable to those used

to protect this information in production environments against unauthorized access, copying, or viewing. In addition, policy should require that before such data is moved or copied to a nonproduction environment it needs to be irreversibly redacted or masked so it is no longer sensitive. Two important considerations during the masking process are (1) to ensure that each resulting data element is realistic in matching the format of the corresponding source data element and (2) that referential integrity is maintained across relational databases so that the same data element is masked in the same manner across instances.

Persistent access by developers to production systems for debugging purposes should be disallowed and replaced by the use of emergency IDs, which are emergency temporary accounts used in a support capacity allowing access to a controlled information system. In order to minimize the inherent loss of efficiency in continually issuing special IDs for certain access purposes, the organization should implement a provisioning process that includes specific authorization criteria, predefined access profiles, predefined primary and proxy approvers, and strict time-limited access.

Physical Access

Physical safeguards, policies, and procedures should be implemented to limit physical access to sensitive information, systems, related facilities, and equipment from unauthorized intrusion as well as natural and environmental hazards.

Physical security risks can be mitigated through zone-oriented implementations, which are physical areas with differing security requirements, which are a function of the sensitivity of the data contained or accessible through the zone and the information technology. The requirements for each zone should be determined through the risk assessment.

Policies and procedures should specify the methods used to control physical access to restricted areas, ensure that access rights are defined based on business need, and that individuals with authorized access are identified by title and/or job function. Management should review the lists of individuals with physical access on a scheduled basis. The access procedures should also cover special access during disaster recovery or emergency mode operations.

Access procedures should include visitor controls, such as sign-in access logs, visitor badges, and escorts by authorized personnel. Where appropriate, physical safeguards should be implemented for individual workstations accessing sensitive data.

Other physical control considerations include:

- **Power** Stable and uninterruptible power supply for all critical components, including automated emergency shutoff due to a device-specific or endemic malfunction.
- **Environmental Management** Regulated temperature and humidity controls as well as automated administrator notification in case indicators deviate from a specified range.
- **Fire Suppression** Fire detection and suppression devices and systems that are automatically activated in the event of a fire. The devices should provide automatic notification of any activation to the organization and emergency responders.
- **Water Damage** Protection from water damage by ensuring that master shutoff valves are known, accessible, and working properly. Additional measures can include raised flowing for critical equipment.

For outsourced datacenters, audits should ensure that the third-party provider has implemented the required security practices and has appropriately secured all organizational infrastructure documentation.

Application and data processing functionality can also be offered by hardware and software located in various user departments. These are commonly housed throughout the organization without special security or environmental controls, and are thus less secure than devices and applications located in a data center or server room. In such situations, overall building or work area security becomes more important. The level of security should depend on the sensitivity of the data that can be accessed and on the significance of applications.

Activity Logging and Monitoring

Activity logging and monitoring will help assess policy compliance, identify intrusions and breaches, and support an effective response program. The degree of logging and monitoring is risk-driven and increases with data accessibility sensitivity.

Activity Monitoring

Systems and databases should log and monitor user activity performed. The scope and level of audit logging and analysis activity will depend on the sensitivity of and risk

associated with the particular data or system, and should be expanded whenever there is an indication of increased risk to assets.

Logs capture data and process events through log entries denoting information such as log on and log off times, the party accessing the sensitive data, access or change occurrences with their date and time, and success or failure indication.

They can provide a record of access and authentication events, configuration changes that can compromise data confidentiality and integrity, and record details of inbound and outbound data transmission traffic.

All activity logs should be reviewed and analyzed by the account owner or designated administrator on a scheduled basis for indications of inappropriate or unusual activity, and suspicious activity or suspected violations should be investigated.

In addition to actual review and analysis, certain logging systems can develop statistical profiles of user access behavior on a continual basis and detect anomalous activity based on the profile.

Logging policies should include guidelines for log review intervals, retention standards, and response time expectations.

Baseline Logging

Organizations should implement a baseline level of logging on all system and database activity, and a higher baseline level of logging on critical systems and databases. This should include high risk activities such as privileged account and administrative-level behavior, direct access to sensitive data stores, privilege escalation, failed login attempts, and failed database operations. Automated triggers should be set to alert appropriate personnel of unusual activities with security implications. All sensitive systems and databases should be checked on a scheduled basis to verify that logging is functioning properly and adheres to standards.

Centralized Log Management

To facilitate the review and analysis of the logs, a copy of audit information from various devices, systems, and databases should be consolidated into a centralized log management repository which will aggregate, normalize, and provide reports and queries. Having all pertinent log entries available in one place and format will help identify policy violations, internal and external data and system compromise, and provide the foundation for forensic analysis.

Centralized logging will greatly facilitate event correlation, since the various logs may each contain indications of the same event or activity.

This consolidation also provides an element of redundancy should any log data become corrupted, provides secure storage for logs, and reduces the impact of log unavailability in the case of a compromised system or database.

Protection of Log Files

Whether at the source system or database or at the aggregate repository, the audit information should be protected from unauthorized access, modification, and deletion. This can be accomplished by limiting audit log access to those with a job-related need and promptly backing up audit log files to a centralized log server or media that is difficult to alter. Attention should also be paid to ensure that sensitive data is not included in the log.

Since malicious technical insiders may attempt to conceal their actions by altering system or database logs, organizations should architect their systems for log integrity. Any direct access to logs should occur by designated security principals through multifactor authentication. Additionally, events should be audited for both success and failure to determine whether any attempts are made to erase the contents of a log.

Storage

Policy should be defined for the storage, overwriting, and maintenance of all event logs, especially on how to deal with full event logs. In order to facilitate any subsequent investigations of data security incidents, sufficient audit record storage capacity should be allocated and auditing should be configured to reduce the likelihood of such capacity being exceeded. This will ensure that logging information is not overwritten and that the audit logs are retained for a period of time consistent with organizational, regulatory, and legal record retention policies. In addition, log retention may be helpful in analysis because older log entries may indicate incident precursor activity or previous undetected instances of similar compromise.

Software Assurance

A significant number of reported security incidents result from exploits against defects in the design or code of software. Software can contain erroneous or intentional code that introduces vulnerabilities and security risks into systems and applications. These hidden access points can provide unauthorized access to systems or data, unauthorized communications capabilities, and unauthorized abilities to change the software.

Ensuring the integrity of internally developed and purchased software will help protect the infrastructure from threats and vulnerabilities and reduce the overall risk of data compromise. To ensure system confidentiality and integrity, it is critical that provisions be included for built-in security of the developed or acquired software by considering the development process, the source code, and the history and reputation of the developers or vendors.

One of the organizational objectives of a Software Assurance Program is to shift the software security stance from patch management to software assurance. Security awareness during development allows designers and developers to apply security principles throughout all the phases of the Software Development Life Cycle and can raise overall software quality and security from the start rather than through the reliance on applying patches after vulnerabilities have been identified.

Software assurance encompasses the following components:

- **People** Education and training for developers and users.
- **Processes** Guidelines and best practices for the development of secure software.
- **Technology** Tools for evaluating software vulnerabilities and quality.
- **Acquisition** Specifications and guidelines for acquisition and outsourcing.

From the process perspective, several security considerations need to be taken into account during system development or purchase. Each phase should assess the business impact of unauthorized disclosure or accidental or deliberate corruption or deletion of business information. Specifically, considerations include security, control, and privacy issues during the requirements and design phase; the implementation of appropriate access controls, audit trails, and activity logs during the development phase; and thorough data security testing during the test phase. A primary testing objective is to ensure that sensitive information is not displayed in a manner where a user can view or access information that they are not authorized to view or access. Additionally, attention should be paid to data migration to ensure that sensitive data is not inadvertently disclosed and that all data is correctly mapped.

For purchased software, all vendor default settings, accounts, and passwords should be changed since these passwords and settings may be generally well known and easily determined via public information. All unnecessary services, protocols, or other functionality should be disabled.

As a necessary best practice, the organization should ensure that the development and testing environments are separate from the production environment. Applications that have been tested thoroughly and are functionally complete can be promoted to the production environment by following the organization's promotion process. Additionally, separation of duties should be implemented between development, test, and end user personnel.

Once a system has been rolled out and operating, the organization should continuously monitor performance to ensure that security controls are effectively implemented and that they remain consistent with preestablished security requirements.

An important software assurance issue is web security. Poorly tested web sites can allow unexpected inputs to pass and weaken security measures. An additional vulnerability exists at the process level since organizations cannot usually train external users or clients accessing their web sites in the basics of access control and security. Particular attention should be paid to thorough testing of web sites and applications on the access, error handling, confidentiality, and integrity levels.

Change Management

Change Management is the process by which changes to systems and databases are managed and documented. The primary objective is to maintain the integrity of the data and system while providing an orderly process for implementing changes needed by organizational units. Weak change management procedures can corrupt systems and data and can introduce new vulnerabilities.

Secure and managed environments require that implementation of changes be predictable and repeatable, following a controlled process that is defined, monitored, and enforced. A successful change management strategy combines internal processes, clearly defined personnel roles, and tools for managing the change process. Risk mitigation is an important part of the change management methodology and the results and effects of changes should be evaluated with an assessment of the risks involved.

The organization should develop and document formal change management procedures covering both normal and emergency changes to systems processing sensitive information. The procedures should include the following requirements:

- All changes are initiated through formal change requests, which include specific requirements, scope, justification, and authorized approvals.

- After you initiate a change request, the effects that the change may have on the system, data, or other interrelated systems are evaluated.
- Responsibility and accountability for creation, approval, and application is segregated.
- Business and technical risks are assessed prior to change implementation and a priority assigned based on urgency, potential benefits, and the ease with which changes can be implemented.
- A Security Impact Analysis is conducted to determine the extent to which changes to data or systems will affect the security posture of the data or systems.
- Any parties affected by the change are notified prior to change implementation.
- All changes are tested in a test environment prior to production implementation.
- Back-out procedures should be developed for all significant changes prior to rollout.
- An emergency change process is operational for emergency changes.
- Changes are monitored to assess the efficacy of change management policies.

A change management process can also be key in distinguishing benign from malicious activity during data breach incidents, since it will allow the response team to use change management information to verify rapidly whether suspicious indications are caused by authorized activity or by an actual event.

Backup and Restore

An organizational data backup and restore process is implemented to copy production data preemptively for restoration purposes in the case of an event that results in the loss or compromise of the data. Restoring the integrity of compromised data will be performed from a verified and validated backup source after an accidental deletion or corruption of data, hardware failure, or facilities damage affecting the storage device.

Strategies for data backup and appropriate backup methodologies are based on the criticality of the data. The primary risk is the inability to recover the data in case of a disaster or other disruptive event. This can be caused by incomplete or sporadic

performance of backup procedures, unreliable backup media, or the inability to access off-site backup material. Written standards should document backup procedures, delineate specific responsibilities, and ensure uniform performance throughout the organization.

Backup best practices include the following:

- Full or incremental data backups should be performed on a daily basis.
- Monthly backup cycles should be maintained for archival purposes and to allow restoration from a clean slate in case a past corruption or compromise is not detected for a long period of time.
- The backup media should be stored in a secure location limited to authorized personnel.
- The backup media should rotated offsite on a weekly basis using a third-party provider.
- The backup system should provide an automatic indication or notification of successful or unsuccessful backup.
- A daily exception report of backup failures should be reviewed and issues resolved on a timely basis.
- Backups should be tested on a quarterly basis for recoverability, including reloading all backed up data and identifying any missing resources that are required to successfully complete the recovery.

A distinction should be drawn between Backup and Restore and data archiving, which refers to the process of long-term storage of inactive data for regulatory or record retention purposes.

Disaster Recovery/ Business Continuity Planning

Effective disaster recovery/business continuity planning (DR/BCP) establishes the basis for an organization to maintain and recover business processes when operations have been disrupted unexpectedly. Its objectives are to minimize financial loss; maintain ongoing operations; and mitigate the strategic, reputational, operational, financial, and legal effects of the disruption.

Events that trigger the implementation of a business continuity plan may have significant security implications, and business continuity plans should be reviewed and tested as an integral part of the security process. Risk assessments should consider the risks that appear in business continuity scenarios and the security posture that may be established.

Business continuity plan review should include the following security considerations:

- Security at the alternate facility.
- Physical and logical access controls for the new production systems and databases as well as for the inactive systems and databases when processing is transferred temporarily to an alternate facility. These controls must be defined for both users and administrators.
- Access provisioning and review methods for users during the emergency.
- Changes in the effectiveness of automated controls such as firewalls and intrusion detection systems due to resource availability and facility and systems changes that may exist when alternate facilities are placed in use.
- Changes in the effectiveness of security processes such as incident response planning under these circumstances.

Disposal

Once sensitive information is no longer needed for a particular business purpose, and once a mandatory retention period has expired, appropriate disposal practices should be implemented to prevent unauthorized access to or use of the information by preventing it from being practicably retrieved. Disposal and media sanitization practices should provide reasonable assurance, in proportion to the confidentiality of the information, that the information cannot be read or reconstructed. Disposal encompasses not only the discarding or abandonment of the information, but also the sale, donation, or transfer of any medium upon which the information is stored.

Sanitization is the process used to remove information from information system media. Sanitization techniques—including clearing, purging, and destroying media information—prevent the disclosure of organizational information to unauthorized individuals when such media is reused or disposed.

Measures

Disposal measures will be based on the sensitivity of the information, the nature and size of the organization's operations, the costs and benefits of different disposal methods, and relevant technological changes. Measures will include shredding, burning, or pulverizing paper records and destruction or erasure of storage media. Media sanitization techniques can be used to ensure that residual data does not remain on media after erasure and cannot be retrieved or reconstructed.

Responsibility

This means designating a single individual, department, or function to be responsible for disposal facilitates accountability and promotes compliance with disposal policies. Depending on the amount and sensitivity of the information to be disposed, it might be advisable to enter into and monitor compliance with a contract with another party engaged in the business of record destruction to dispose of material in an appropriate manner. The competency and integrity of the disposal company can be determined through the review of an independent audit of its operations and references from reliable sources.

Recording

Where practical, the disposal of sensitive data should be logged in a Record of Destruction or similar form, including the party responsible for and performing disposal, the date, medial type, and method of disposal.

Insiders

Insiders have a significant advantage over external parties in the ability to access and use sensitive organizational information in an unauthorized manner. They have or can more easily gain the knowledge to bypass security measures designed to prevent unauthorized access. They may also be aware of flaws and vulnerabilities in internal processes and technology. Insider attacks fall into the following categories:

- **Sabotage** This can be performed by current or former employees or contractors who intentionally exceed or misuse an authorized level of access with the intention of harming a specific individual, group, or the organization. These insiders are usually disgruntled employees motivated by a desire for revenge for a perceived or actual negative event such as termination, supervisor disputes, transfers or demotions, and salary or pay dissatisfaction.

- **Fraud** Insiders who commit fraud with the intention of deceptively obtaining a certain gain are usually motivated by financial considerations, either for direct additional income or in return for payment from another party.
- **Theft of sensitive information** These insiders may be motivated by the financial gain accruing from using the information in a fraudulent manner. Others may be disgruntled employees who choose to embarrass employers by revealing the information.
- **Compromises due to carelessness or negligence** Data breaches due to insiders can be caused by careless employees or well-meaning users who lack the necessary security training and awareness for their job function. Users who have legitimate access to information may not exercise due care and inadvertently share this information with unauthorized parties. Even though fraud or theft is unlikely to result from data leakage under these circumstances, the prevalence of these types of breaches can eventually result in a significant incident.

Insider attacks usually involve unauthorized access either directly or through a compromised user or administrative account, shared account, or system account. These compromises can be detected due to system irregularity, nontechnical means such as notification by other employees or customers, and log review. They can be prevented through a layered approach consisting of policy and technical control enforcement. The following practices will help reduce the risk of insider attacks:

- **Segregation of duties** Separation and division of certain areas of responsibility for critical functions among multiple employees to reduce the opportunity for unauthorized modifications or misuse by limiting the possibility that one individual could commit unauthorized actions without the cooperation of another individual within the organization. By segregating duties, the organization will minimize the risk that a combination of functions under the responsibility of a single individual can be combined to result in a security violation.
- **Rotation of duties** This control, similar in concept to segregation of duties, is intended to prevent or detect misuse by minimizing over-dependence on a single staff member, thus increasing the probability of detecting policy violations or actual fraud.

- **Least privilege** The minimum privilege and resource access required to fulfill the person's job function. This limits the scope of possible threats by reducing the number of privileges that may potentially be abused.
- **Log monitoring** System or database log monitoring and review will help detect unauthorized access, even though consideration must be given to the fact that attempts may be made to conceal actions by modifying the logs.
- **Administrative account control** The use of administrative or privileged accounts should be closely managed and logged, and shared privileged accounts should be disabled.
- **Effective access provisioning and review** The provisioning process should include an efficient mechanism for updating access levels when a user's status or role changes. This is especially relevant upon user termination, where all internal and external access control privileges should be revoked in a prompt manner.

Social Engineering

Social engineering is any manipulation of a person, usually through social interaction, to obtain unauthorized information. By using persuasion, aggression, or other interpersonal skills, the unauthorized party will attempt to encourage a legitimate user or other authorized party to provide sensitive information or authentication credentials.

Risks associated with social engineering can be mitigated through a security program that includes ongoing awareness and training, as well as effective policies and procedures for employees, vendors, and partners. The challenge is to encourage a security culture that is collaborative, structured, and ingrained throughout the organization's processes and people without fostering an unnecessary level of distrust.

Training can help employees understand the potential risk of social engineering threats, provide them with the tools they need to recognize and respond to these threats, and understand why their role within the security culture is vital to organizational health. Employees in higher risk positions such as help desk staff and system administrators may benefit from specialized training.

In addition to training, strong third-party identification procedures should be implemented, especially for employees that interact with external parties. These will be used to properly authenticate the identity of the other person prior to engaging in a discussion about confidential information. This may include requesting identification information at more than one juncture during the conversation.

Third-Party Vendors

Organizations are increasingly using vendors and service providers for a variety of services, such as data center and network operations, HR and payroll, data backup, and remote help desk. Some of these services require that the vendors and third parties access, maintain, process, or are otherwise permitted access to confidential information, including an organization's sensitive customer and employee data, creating a situation where vendors essentially have the same access to this information as authorized internal employees.

Because a significant number of sensitive data breaches occur through the access to this data by outside parties, and due to heightened regulatory concern, vendor selection and supervision must become integral parts of organizational risk management strategies, especially since outsourcers typically serve multiple clients and may have security implementations that do not adequately take into account the value of the information.

The organization should exercise appropriate due diligence in selecting its service providers, including developing a process to perform vendor risk assessments based on the criticality and sensitivity of the outsourced process and data. This should include importance of the outsourced function, the nature of the activities the vendor will perform, and the inherent risk of each activity.

To ensure proper management of the due diligence process, a questionnaire can be developed covering vendor history, financial condition, personnel practices, information security policies and procedures, business continuity, and other relevant areas. This will ensure that all key areas of the due diligence process are addressed in a uniform manner.

Once a vendor has been selected, the organization should:

- Review and approve the service provider's information security policy and program.
- Enter into and enforce a contract with the service provider that requires the implementation of appropriate measures designed to protect against unauthorized access to or use of sensitive information accessed or maintained by the service provider. These include security controls for the protection of sensitive information, limiting data access to authorized staff, and defining the way in which the vendor is permitted to further outsource to other third parties.

- Include in the contract the requirement that the service provider take appropriate actions to address incidents of unauthorized access to the organization's sensitive data, including notification to the organization as soon as possible following any such incident.
- Monitor its service providers to confirm they are satisfying their contractual obligations through audits and reviews conducted by qualified internal or external independent parties. Vendor security assessment must be performed when the vendor begins performing functions that have access to confidential information and on a scheduled basis thereafter, usually yearly. They must be reperformed before the next scheduled review basis in case of a vendor security incident, changes in infrastructure or information technology platform used to process confidential information, or the use of subcontractors not previously identified by the third party that have been granted access to confidential information.
- Where a sufficient level of trust cannot be established in the external services and/or service providers, the organization should employ compensating security controls or under certain circumstances accept the greater degree of risk to its operations and information assets.
- Take steps to cure a violation or terminate the contract if the organization determines that the third-party vendor has violated a material term of the contract regarding information security.
- Upon termination of the outsourcing contract, ensure that the third-party vendor returns or destroys without maintaining any copies all sensitive information received from, created, or received on behalf of the organization. If such a return or destruction is not feasible, the vendor must extend the protections of the contract and limit further uses and disclosures for as long as the information is maintained.

An additional level of caution and consideration should be exercised if security services themselves are outsourced to obtain greater expertise, a greater range of services, or to decrease cost. Since the organization retains the same responsibilities for security as if those services were performed internally, it should ensure it has sufficient expertise to oversee and manage an outsourced security service relationship, both on a contract level for contract compliance and on a security level to sufficiently understand the scope and nature of the service, react in a timely manner when the services provided are not at the

appropriate level, no longer coordinate with the internal security controls, or no longer provide the risk mitigation desired.

Training and Awareness

Effective training in data security and privacy practices, both on an initial and refresher basis, is a critical component of the information security program and is essential for ensuring that employees can effectively adhere to and carry out policy.

Establishing and maintaining a robust and relevant information security awareness and training program as part of the overall information security program is the primary conduit for providing employees with the information and tools needed to protect the organization's information assets. It will help teach users how to protect the confidential information that has been entrusted to them. In addition, it is critical to timely breach response in the event of a breach or compromise.

Training programs will help create a culture of security appropriate for the organization as determined by an enterprisewide risk assessment and tied to the organization's mission, values, and critical assets.

The organization should develop, disseminate, and periodically review and update a formal documented security awareness and training program that addresses purpose, scope, roles, responsibilities, and compliance. In addition to the general data security training and awareness, programs can also be developed for particular systems or data stores.

On a general level, a training program should encompass the following:

- The organization's vision and mission relating to the protection of information resources, including the importance of information security and the ways in which it forms part of critical asset protection.
- Applicable laws, regulations, policies, and procedures.
- Data classification requirements.
- Data life cycle security considerations, including limiting the data that is collected, accessed, or displayed to that which is essential for the function to be performed, data protection during usage, processing, and storage, and effective methods of disposal.
- An overview of risks and safeguards.

- Roles and responsibilities, including clear guidelines on the correct use of the organization's information and what each particular group of users is authorized to access.
- The implication of security incidents to both the organization and the individual.
- Reporting requirements and procedures for unauthorized access, disclosure, or modification of information.
- An overview of the data security incident management program, including workflow and other relevant features.

Training can be conducted in a classroom setting, remotely, and periodic issuance of security awareness literature. Training and awareness material can also be made available on internal networks that can be accessed by employees.

The training program should distinguish between audiences since not everyone needs the same degree or type of information security awareness. In addition to general data security issues, training programs can be developed for:

- End users about existing policies and procedures in order to provide a sound basis of understanding before granting access to sensitive information.
- Remote or mobile users.
- Specific departments or groups with security sensitive positions as well as specific systems.
- IT development and support personnel with technical security training needs, including planning and implementing security for new systems that will use sensitive information.
- Information security and audit staff who are tasked to implement or review security policies and procedures.

An effective security awareness and training program requires proper planning, implementation, maintenance, and periodic evaluation, including scope definition and objectives, program development, administration, and periodic evaluation.

Once the program has been implemented, a process to monitor compliance and effectiveness should be designed to capture key information on program activity. This will allow an assessment of the program as to its adherence to established goals and standards. Gap identification will drive any corrective action, which may take the

form of formal reminders and additional awareness and training. Security awareness surveys can also measure the awareness level and highlight any areas needing improvement.

Compensating Controls

If a prescribed or recommended control cannot be effectively implemented or would cause adverse impact that would not be offset by the reduced risk, it may be necessary to specify and employ compensating controls, which are employed in lieu of a recommended control and provides equivalent or comparable protection for the data.

The effectiveness of a compensating control is dependent on the specifics of the environment in which the control is implemented, the surrounding security controls, and the configuration of the control. Compensating controls must meet the intent and rigor of the original control requirement and be commensurate with the additional risk imposed by not adhering to the requirement.

If a compensating control is implemented, the data owner should provide a rationale of the decision and a description and justification of the manner in which the control provides an equivalent security capability or level of protection. This is accomplished through Risk Acceptances (RAs), which describes the risks, the reasons for the lack of compliance, a justification for why the exception is warranted, the compensating controls implemented to address the risk, the expiration date of the exception, and review procedures.

Auditing

Risk-based audit programs should be conducted by internal and/or external auditors to ensure the adequate implementation and effectiveness of data security policies and procedures. Audits involve the review of existing controls with the objective to provide management assurance that the controls implemented are effective and to report any deficiencies together with the appropriate recommended actions.

In addition to possessing the appropriate skills and experience, auditors should be independent from the unit or organization being audited to ensure unbiased results and opinions. To minimize disruptions to business activities, the scope, approach, and timing of the audits should be planned and agreed with appropriate management.

Auditors should conduct sufficient review in the following areas to provide a basis for evaluating the overall data security program.

Data Security Policy

- Does the organization have a written data security policy?
- Has the policy been approved by upper level management?
- Are the scope and contents of the policy appropriate given the size and complexity of the organization and its operations?
- Does the policy contain the objectives of the program, assign responsibility for implementation, and provide methods for compliance and enforcement?
- Is the policy periodically updated to reflect changes in the operations, processes, and systems, as well as changes in the threats or risks to the organization's sensitive information?
- Does the organization report to its board or an appropriate committee of the board at least annually on the overall status of the information security program?

Risk Assessment

- Has all sensitive data been identified, including location and methods for storage, processing, transmission, and disposal?
- Has all sensitive data been classified?
- Has all sensitive data been assigned a data owner?
- Have reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of sensitive information been identified?
- Has the organization assessed the likelihood and potential damage of these threats?
- Does the organization update the risk assessment on a scheduled basis?
- Additionally, does the organization update the risk assessment prior to major changes to data, systems, or new external conditions?

Controls

- Have measures been taken to limit the amount of sensitive information collected, maintained, or processed to the minimum amount necessary for a particular business purpose?

- Are there appropriate logical and physical access controls on sensitive data?
- Are the concepts of least privilege and segregation of duties considered when granting access to sensitive information?
- Is sensitive data encrypted during transmission or in storage?
- Has a change management process been implemented to ensure that modifications to sensitive systems are consistent with the organization's information security program?
- Have third-party and vendor controls been implemented for any third party collecting, accessing, or processing sensitive information?
- Are monitoring and logging procedures in place to detect unauthorized access to sensitive information?
- Has a breach response program been developed and staffed in cases where the organization suspects or detects unauthorized access to sensitive information, including appropriate notification to affected parties and regulatory agencies?
- Have employees been trained to implement the data security program?

Testing

- Does the organization regularly test the effectiveness of key controls, systems, and procedures of its information security program?
- Are tests conducted by independent staff or are test results reviewed by independent staff?

Third Party Providers

- Does the organization provide or allow access to sensitive information to any third-party service providers?
- For third-party providers with access to sensitive information, has the organization conducted appropriate due diligence in the selection process, taking into consideration data security?
- Are third-party providers with access to sensitive information required by contract to implement appropriate information security programs and measures?
- Does the organization monitor its third-party providers with access to sensitive information to confirm that they are maintaining appropriate security measures to safeguard the organization's sensitive information?

Testing

An information security program should include regular testing of key controls, systems, and procedures in order to obtain assurance and confidence that the security implemented controls are operational and effective in their application. Testing will determine the extent to which the controls are implemented correctly, operate as intended, and produce the desired outcome with respect to meeting data security requirements. This review is designed to identify control weaknesses, identify actions that are needed to correct these weaknesses, monitor the implementation of necessary corrective actions, and periodically assess or test the adequacy of controls.

The frequency and nature of the testing is determined by the risk assessment and adjusted as necessary to reflect changes in both internal and external conditions. Testing is based on a test plan, which includes the list of controls to test, a timeline, testing responsibility, and testing methods, including the actual testing instructions or test scripts. The number and complexity of the test scripts will be determined by the organizational size and complexity as well as by data sensitivity and risk.

Control testing occurs by reviewing samples of the control. Table 3.1 is the recommended sample size for test documentation based on control frequency.

Testing exceptions should be documented, noting whether the test failed due to design or operational deficiency. Upon investigation of each exception, remediation actions should be initiated. These are guided by a plan of action that documents planned, implemented, and evaluated remedial actions to correct deficiencies noted during the assessment and testing of the security controls and to reduce or eliminate known vulnerabilities. Controls should be retested upon completion of the remediation effort once a sufficient sample population becomes available.

The tests should be conducted by staff independent of those that develop or maintain the security program. Whether third parties should be used to either conduct tests or review their results will generally depend on regulatory compliance regulations, previous audit processes and results, whether independent organizational resources are available, and general expense and reliability considerations.

Testing documentation should be maintained for activities conducted in connection with internal control reviews, testing and remediation actions. The documentation should include the personnel involved in the test, the key factors considered, the evaluation methods used, and the conclusions reached. Documentation should be of sufficient detail to permit effective supervisory or oversight review. Independent reviewers should be able to examine and understand the documentation and determine how the original reviewers reached their conclusions.

Table 3.1 Control Testing Sample Size

Frequency of Control	Sample Size
Daily	25
Weekly	12
Semimonthly	5
Monthly	3
Quarterly	2
Semi-Annually	2
Annually	1
Automated	1
Recurring (multiple times a day)	40

Updating

In this section we'll discuss actions organizations should take to ensure that their security is up-to-date.

Security Program

The organization should review and reevaluate its security program on a scheduled basis to determine the extent of any required adjustments to its components. It will need to consider the scope, impact, and urgency of any new or changing threat or vulnerability and any changes to the information sensitivity in order to reassess possible risk and update the security process and controls accordingly.

More systemic events like mergers and acquisitions, new business endeavors, outsourcing agreements, new critical systems, or updates to existing systems will warrant an immediate review prior to the normal scheduled review.

Controls

The implementation of effective controls and safeguards is an ongoing process, whereby the effectiveness of controls at a specific point in time is just one indicator of the overall security framework. A program to audit, reassess, and update controls and safeguards on a regular basis allows the organization to react effectively to changing vulnerabilities, technologies, and business processes and conditions.

Summary

- A data security program will allow the management of data security risks and can limit the organization's vulnerability to data compromise.
- The data security program includes data classification, risk assessment, risk mitigation strategy, controls to protect the data, monitoring and testing of the controls to verify that they are effective, and a process to continuously gather and analyze new threats and vulnerabilities.
- Information security controls are the technical, physical, administrative, and policy safeguards designed to protect sensitive data.
- As part of a Defense in Depth strategy, a variety of controls are necessary for a comprehensive and robust security framework.
- Lost or stolen laptops represent a significant source of data compromise. If sensitive data must be stored on a laptop, full-disk encryption should be used to prevent unauthorized parties from retrieving the data.
- The small size of portable storage devices such as flash drives increases the possibility of physical loss with the attendant data loss.
- The organization should evaluate all transfers of physical media containing sensitive information to discontinue unnecessary or redundant transfers. Sensitive data in transport should be encrypted.
- An e-mail acceptable use policy should be implemented to clearly describe applicable restrictions on the transmission of sensitive information via e-mail.
- A variety of technical safeguards should be used for data security, including firewalls, intrusion detection systems, and vulnerability scanning.
- Sensitive data transmission should be performed only over a trusted path or medium with cryptographic controls.
- The organization should implement policies and processes governing the conditions under which remote access is granted and terminated, and all communications should be through a virtual private network that can provide a secure communications channel across a public network.
- All servers and workstations should be configured with antivirus software that is automatically updated on a daily basis with new virus definitions.

- Organizations should have an effective process for adding, modifying, and removing user access to data resources.
- Passwords should adhere to complexity and aging requirements.
- Periodic assessments and reviews of entitlement privileges and permissions to systems and data should be performed.
- Privileged and administrative accounts should be tightly controlled.
- Persistent update access by developers to production systems should be removed and read access should be granted on a case-by-case basis.
- Physical safeguards, policies, and procedures should be implemented to limit physical access to sensitive information, systems, related facilities, and equipment.
- Activity logging and monitoring will help assess policy compliance and identify intrusions and breaches.
- Each phase of the Software Development Life Cycle should assess the business impact of unauthorized disclosure or accidental or deliberate corruption or deletion of business information.
- The organization should develop and document formal change management procedures covering both normal and emergency changes to systems processing sensitive information.
- Once sensitive information is no longer needed, appropriate disposal practices should be implemented to prevent unauthorized access to or use of the information by preventing it from being practicably retrieved.
- Practices that will help reduce the risk of insider attacks include segregation and rotation of duties, least privilege, log monitoring, administrative account control, and effective access provisioning and review.
- Risks associated with social engineering can be mitigated through a security program that includes ongoing awareness and training, as well as effective policies and procedures for employees, vendors, and partners.
- Vendor selection and supervision must become integral parts of organizational risk management strategies since sensitive data breaches can occur through the access to this data by outside parties.

- Establishing and maintaining a robust and relevant information security awareness and training program as part of the overall information security program is the primary conduit for providing employees with the information and tools needed to protect the organization's information assets.
- Risk-based audit programs should be conducted to ensure the adequate implementation and effectiveness of data security policies and procedures.
- Regular testing of key controls will determine the extent to which they are implemented correctly, operate as intended, and produce the desired outcome with respect to meeting data security requirements.
- The organization should review and reevaluate its security program on a scheduled basis to determine the extent of any required adjustments to any of its components.