Catalog of Control Systems Security: Recommendations for Standards Developers

September 2009

Homeland Security

2.7.11.2 Supplemental Guidance

Electronic signatures are acceptable for use in acknowledging rules of behavior unless specifically prohibited by organizational policy.

2.7.11.3 Requirement Enhancements

The organization includes in the rules of behavior, explicit restrictions on the use of social networking sites, posting information on commercial web sites, and sharing system account information.

2.7.12 Security-Related Activity Planning

2.7.12.1 Requirement

The organization plans and coordinates security-related activities affecting the control system before conducting such activities to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, or individuals.

2.7.12.2 Supplemental Guidance

Routine security-related activities include, but are not limited to, security assessments, audits, system hardware and software maintenance, security certifications, and testing/exercises. Organizational advanced planning and coordination includes both emergency and nonemergency (i.e., routine) situations.

2.7.12.3 Requirement Enhancements

None.

2.8 System and Communication Protection

System and communication protection consists of steps taken to protect the control system and the communication links between system components from cyber intrusions. Although control system and communication protection might logically include both physical and cyber protection, this section addresses only cyber protection. Physical protection is addressed in Section 2.4.

2.8.1 System and Communication Protection Policy and Procedures

2.8.1.1 Requirement

The organization develops, disseminates, and periodically reviews and updates:

1. A formal, documented system and communication protection policy that addresses:
   a. The purpose of the system and communication protection policy as it relates to protecting the organization's personnel and assets
   b. The scope of the system and communication protection policy as it applies to all the organizational staff and third-party contractors
   c. The roles, responsibilities, coordination among organizational entities, and management accountability structure of the security program to ensure compliance with the organization's system and communications protection policy and other regulatory commitments
2. Formal, documented procedures to facilitate the implementation of the control system and communication protection policy and associated systems and communication protection controls.

2.8.1.2 Supplemental Guidance

The organization ensures the system and communication protection policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The system and communication protection policy needs to be included as part of the general information security policy for the organization. System and communication protection procedures can be developed for the security program in general and a control system in particular, when required.

2.8.1.3 Requirement Enhancements

None.

2.8.2 Management Port Partitioning

2.8.2.1 Requirement

The control system components separate telemetry/data acquisition services from management port functionality.

2.8.2.2 Supplemental Guidance

The control system management port needs to be physically or logically separated from telemetry/data acquisition services and information storage and management services (e.g., database management) of the system. Separation may be accomplished by using different computers, different central processing units, different instances of the operating systems, different network addresses, combinations of these methods, or other methods as appropriate.

2.8.2.3 Requirement Enhancements

None.

2.8.3 Security Function Isolation

2.8.3.1 Requirement

The control system isolates security functions from nonsecurity functions.

2.8.3.2 Supplemental Guidance

The control system isolates security functions from nonsecurity functions by means of an isolation boundary (implemented via partitions, domains) that controls access to and protects the integrity of the hardware, software, and firmware that perform those security functions. The control system maintains a separate execution domain (e.g., address space) for each executing process.

Some legacy control systems may not implement this capability. In situations where it is not implemented, the organization details its risk acceptance and mitigation in the control system security plan.

2.8.3.3 Requirement Enhancements

The control system employs the following underlying hardware separation mechanisms to facilitate security function isolation.

1. The control system isolates security functions (i.e., functions enforcing access and information flow control) from both nonsecurity functions and from other security functions.
2. The control system minimizes the number of nonsecurity functions included within the isolation boundary containing security functions.
3. The control system security functions are implemented as largely independent modules that avoid unnecessary interactions between modules.
4. The control system security functions are implemented as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.

2.8.4 Information Remnants

2.8.4.1 Requirement

The control system prevents unauthorized or unintended information transfer via shared system resources.

2.8.4.2 Supplemental Guidance

Control of system remnants, sometimes referred to as object reuse, or data remnants, prevents information, including cryptographically protected representations of information previously produced by the control system, from being available to any current user/role/process that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the system. This control does not address: (1) information remnants that refers to residual representation of data that has been in some way nominally erased or removed, (2) covert channels where shared resources are manipulated to achieve a violation of information flow restrictions, or (3) components in the control system for which only a single user/role exists.

2.8.4.3 Requirement Enhancements

None.

2.8.5 Denial-of-Service Protection

2.8.5.1 Requirement

The control system protects against or limits the effects of denial-of-service attacks based on an organization's defined list of types of denial-of-service attacks.

2.8.5.2 Supplemental Guidance

A variety of technologies exist to limit, or in some cases, eliminate the effects of denial-of-service attacks. For example, network perimeter devices can filter certain types of packets to protect devices on an organization's internal network from being directly affected by denial-of-service attacks.

2.8.5.3 Requirement Enhancements

1. The control system restricts the ability of users to launch denial-of-service attacks against other control systems or networks.
2. The control system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial-of-service attacks.

2.8.6 Resource Priority

2.8.6.1 Requirement

The control system limits the use of resources by priority.

2.8.6.2 Supplemental Guidance

Priority protection helps prevent a lower-priority process from delaying or interfering with the control system servicing any higher-priority process. This control does not apply to components in the system for which only a single user/role exists.

2.8.6.3 Requirement Enhancements

None.

2.8.7 Boundary Protection

2.8.7.1 Requirement

The organization defines the external boundary(ies) of the control system. Procedural and policy security functions define the operational system boundary, the strength required of the boundary, and the respective barriers to unauthorized access and control of system assets and components. The control system monitors and manages communications at the operational system boundary and at key internal boundaries within the system.

2.8.7.2 Supplemental Guidance

Managed interfaces employing boundary protection devices include proxies, gateways, routers, firewalls, guards, or encrypted tunnels arranged in an effective organization-defined security architecture (e.g., routers protecting firewalls and application gateways residing on a protected subnetwork commonly referred to as a demilitarized zone or DMZ). Control system boundary protections at any designated alternate processing/control sites provide the same levels of protection as that of the primary site.

As part of a defense-in-depth protection strategy, the organization considers partitioning higher-impact systems into separate physical domains (or environments) and applying the concepts of managed interfaces described above to restrict or prohibit network access in accordance with an organizational assessment of risk. FIPS 199 security categorization guides the selection of appropriate candidates for domain partitioning.

The organization carefully considers the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may include third party provided access lines and other service elements. Consequently, such interconnecting transmission services may represent sources of increased risk despite contract security provisions. Therefore, when this situation occurs, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk.

2.8.7.3 Requirement Enhancements

1. The organization physically allocates publicly accessible control system components to separate subnetworks with separate, physical network interfaces. Publicly accessible control system components include public web servers. Generally, no control system information should be publicly accessible.
2. The organization prevents public access into the organization’s internal control system networks except as appropriately mediated.
3. The organization limits the number of access points to the control system to allow for better monitoring of inbound and outbound network traffic.
4. The organization implements a managed interface (boundary protection devices in an effective security architecture) with any external telecommunication service, implementing security measures appropriate to the required protection of the integrity and confidentiality of the information being transmitted.
5. The control system denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).
6. The organization prevents the unauthorized release of information outside the control system boundary or any unauthorized communication through the control system boundary when an operational failure occurs of the boundary protection mechanisms.

7. The organization prevents the unauthorized exfiltration of information across managed interfaces.
8. The control system checks incoming communications to ensure that the communications are coming from an authorized source and routed to an authorized destination.
9. The control system at managed interfaces, denies network traffic and audits internal users (or malicious code) posing a threat to external systems.
10. The control system prevents remote devices that have established a nonremote connection with the system from communicating outside that communications path with resources in nonorganization controlled networks.
11. The control system routes all internal communications traffic to the Internet through authenticated proxy servers within the managed interfaces of boundary protection devices.

2.8.8 Communication Integrity

2.8.8.1 Requirement

The control system design and implementation protects the integrity of electronically communicated information.

2.8.8.2 Supplemental Guidance

If the organization is relying on a commercial service provider for communication services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security measures for transmission integrity. When it is infeasible or impractical to obtain the necessary assurances of effective security through appropriate contracting vehicles, the organization either implements appropriate compensating security measures or explicitly accepts the additional risk.

2.8.8.3 Requirement Enhancements

1. The organization employs cryptographic mechanisms to ensure recognition of changes to information during transmission unless otherwise protected by alternative physical measures (e.g., protective distribution systems).
2. The use of cryptography within a control system will introduce latency to control system communication. The latency introduced from the use of cryptographic mechanisms must not degrade the operational performance of the control system or impact personnel safety.
3. Failure of a cryptographic mechanism must not create a denial of service. Control systems generally support the objectives of availability, integrity, and confidentiality. Therefore, the use of cryptography should be determined after careful consideration.
4. The control system maintains the integrity of information during aggregation, packaging, and transformation in preparation for transmission.

2.8.9 Communication Confidentiality

2.8.9.1 Requirement

The control system design and implementation protects the confidentiality of communicated information where necessary.

2.8.9.2 Supplemental Guidance

The use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption. The use of cryptographic mechanisms within a control system could introduce communications latency because of the additional time and computing resources required to

encrypt, decrypt, and authenticate each message. Any latency induced from the use of cryptographic mechanisms must not degrade the operational performance of the control system.

2.8.9.3 Requirement Enhancements

1. The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures.
2. The control system maintains the confidentiality of information during aggregation, packaging, and transformation in preparation for transmission.

2.8.10 Trusted Path

2.8.10.1 Requirement

The control system establishes a trusted communications path between the user and the system.

2.8.10.2 Supplemental Guidance

A trusted path is employed for high-confidence connections between the security functions of the control system and the user (e.g., for login).

Login-to-operator interface should be protected by trusted path or a compensating control. A trusted path is a mechanism by which a person at a terminal can communicate directly with the Trusted Computing Base (TCB) that provides the security functions of the system. This mechanism can only be activated by the person or the TCB and cannot be imitated by untrusted software. The TCB is the totality of protection mechanisms within a computer system—including hardware, firmware, and software—the combination of which is responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system. The ability of a trusted computing base to correctly enforce a security policy depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel of parameters (e.g., a user's clearance) related to the security policy.

2.8.10.3 Requirement Enhancements

None.

2.8.11 Cryptographic Key Establishment and Management

2.8.11.1 Requirement

When cryptography is required and employed within the control system, the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures.

2.8.11.2 Supplemental Guidance

Organizations need to select cryptographic protection that matches the value of the information being protected and the control system operating constraints. A formal written policy needs to be developed to document the practices and procedures relating to cryptographic key establishment and management. These policies and procedures need to address, under key establishment, such items as key generation process in accordance with a specified algorithm and key sizes based on an assigned standard. Key generation must be performed using an effective random number generator. The policies for key management need to address such items as periodic key changes, key destruction, and key distribution in accordance with defined standards.

2.8.11.3 Requirement Enhancements

The organization maintains availability of information in the event of the loss of cryptographic keys by users.

2.8.12 Use of Validated Cryptography

2.8.12.1 Requirement

The organization develops and implements a policy governing the use of cryptographic mechanisms for the protection of control system information. The organization ensures all cryptographic mechanisms comply with applicable laws, regulatory requirements, directives, policies, standards, and guidance.

2.8.12.2 Supplemental Guidance

Any cryptographic modules deployed within a control system, at a minimum, must be able to meet the FIPS 140-2. Assessment of the modules must include validation of the cryptographic modules operating in approved modes of operation. The most effective safeguard is to use a cryptographic module validated by the Cryptographic Module Validation Program. Additional information on the use of validated cryptography can be found at http://csrc.nist.gov/cryptval.

2.8.12.3 Requirement Enhancements

1. The organization protects cryptographic hardware from physical tampering and uncontrolled electronic connections.
2. The organization selects cryptographic hardware with remote key management capabilities.

2.8.13 Collaborative Computing

2.8.13.1 Requirement

The use of collaborative computing mechanisms on the control system is strongly discouraged and, if used, local users are provided an explicit indication of use.

2.8.13.2 Supplemental Guidance

Collaborative computing mechanisms include video and audio conferencing capabilities or instant messaging technologies. Explicit indication of use includes signals to local users when cameras and/or microphones are activated.

2.8.13.3 Requirement Enhancements

1. If collaborative computing mechanisms are used on the control system, they are disconnected and powered down when not in use.
2. The control system or supporting environment blocks both inbound and outbound traffic between instant messaging clients that are independently configured by end users and external service providers.
3. The organization disables or removes collaborative computing devices from control systems in organization-defined secure work areas.

2.8.14 Transmission of Security Parameters

2.8.14.1 Requirement

The control system reliably associates security parameters (e.g., security labels and markings) with information exchanged between the enterprise systems and the control system.

2.8.14.2 Supplemental Guidance

Security parameters may be explicitly or implicitly associated with the information contained within the control system.

2.8.14.3 Requirement Enhancements

The control system validates the integrity of security parameters exchanged between systems.

2.8.15 Public Key Infrastructure Certificates

2.8.15.1 Requirement

The organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.

2.8.15.2 Supplemental Guidance

Registration to receive a public key certificate needs to include authorization by a supervisor or a responsible official and needs to be accomplished using a secure process that verifies the identity of the certificate holder and ensures that the certificate is issued to the intended party.

2.8.15.3 Requirement Enhancements

Any latency induced from the use of public key certificates must not degrade the operational performance of the control system.

2.8.16 Mobile Code

2.8.16.1 Requirement

The organization:

1. Establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the control system if used maliciously
2. Documents, monitors, and manages the use of mobile code within the control system. Appropriate organizational officials authorize the use of mobile code.

2.8.16.2 Supplemental Guidance

Mobile code technologies include Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance need to apply to both the selection and use of mobile code installed on organizational servers and mobile code downloaded and executed on individual workstations. Control procedures need to prevent the development, acquisition, or introduction of unacceptable mobile code within the control system. Additional information on risk-based approaches for the implementation of mobile code technologies can be found at http://iase.disa.mil/mcp/index.html.

2.8.16.3 Requirement Enhancements

The control system implements detection and inspection mechanisms to identify unauthorized mobile code and takes corrective actions, when necessary.

2.8.17 Voice-Over Internet Protocol

2.8.17.1 Requirement

The organization: (1) establishes usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the system if used maliciously and (2) authorizes, monitors, and controls the use of VoIP within the control system.

2.8.17.2 Supplemental Guidance

Generally, VoIP technologies should not be employed on control systems.

2.8.17.3 Requirement Enhancements

None.

2.8.18 System Connections

2.8.18.1 Requirement

All external control system and communication connections are identified and protected from tampering or damage.

2.8.18.2 Supplemental Guidance

External access point connections to the control system need to be secured to protect the system. Access points include any externally connected communication end point (for example, dialup modems) terminating at any device within the electronic security perimeter. The first step in securing these connections is to identify the connections along with the purpose and necessity of the connection. This information needs to be documented, tracked, and audited periodically. After identifying these connection points, the extent of their protection needs to be determined. Policies and procedures need to be developed and implemented to protect the connection to the business or enterprise system. This might include disabling the connection except when specific access is requested for a specific need, automatic timeout for the connection, etc.

2.8.18.3 Requirement Enhancements

None.

2.8.19 Security Roles

2.8.19.1 Requirement

The control system design and implementation specifies the security roles and responsibilities for the users of the system.

2.8.19.2 Supplemental Guidance

Security roles and responsibilities for control system users need to be specified, defined, and implemented based on the sensitivity of the information handled by the user. These roles may be defined for specific job descriptions or for individuals.

2.8.19.3 Requirement Enhancements

None.

2.8.20 Message Authenticity

2.8.20.1 Requirement

The control system provides mechanisms to protect the authenticity of device-to-device communications.

2.8.20.2 Supplemental Guidance

Message authentication provides protection from malformed traffic from misconfigured devices and malicious entities.

2.8.20.3 Requirement Enhancements

Message authentication mechanisms should be implemented at the protocol level for both serial and routable protocols.

2.8.21 Architecture and Provisioning for Name/Address Resolution Service

2.8.21.1 Requirement

The control system's devices that collectively provide name/address resolution services for an organization are fault tolerant and implement address space separation.

2.8.21.2 Supplemental Guidance

In general, do not use domain name system (DNS) services on a control system. Host-based name resolution solutions are the recommended practice. However, if DNS services are implemented, deploy at least two authoritative DNS servers. The DNS configuration on the host will reference one DNS server as the primary source and the other as the secondary source. In addition, locate the two DNS servers on different network subnets and separate geographically. If control system resources are accessible from external networks, establish authoritative DNS servers with separate address space views (internal and external) to the control system resources. The DNS server with the internal view provides name/address resolution services within the control system boundary. The DNS server with the external view only provides name/address resolution information pertaining to control system resources accessible from external resources. The list of clients who can access the authoritative DNS server with a particular view is also specified.

2.8.21.3 Requirement Enhancements

The use of secure name/address resolution services must not adversely impact the operational performance of the control system.

2.8.22 Secure Name/Address Resolution Service (Authoritative Source)

2.8.22.1 Requirement

The control system resource (i.e., authoritative DNS server) that provides name/address resolution service provides additional artifacts (e.g., digital signatures and cryptographic keys) along with the authoritative DNS resource records it returns in response to resolution queries.

2.8.22.2 Supplemental Guidance

In general, do not use DNS services on a control system. Host-based name resolution solutions are best practice. This requirement enables remote clients to obtain origin authentication and integrity verification assurances for the name/address resolution information obtained through the service. A DNS server is an example of control system resource that provides name/address resolution service; digital signatures and cryptographic keys are examples of additional artifacts; and DNS resource records are examples of authoritative data.

2.8.22.3 Requirement Enhancements

The control system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains.

2.8.23 Secure Name/Address Resolution Service (Recursive or Caching Resolver)

2.8.23.1 Requirement

The control system resource (i.e., resolving or caching name server) that provides name/address resolution service for local clients performs data origin authentication and data integrity verification on the resolution responses it receives from authoritative DNS servers when requested by client systems.

2.8.23.2 Supplemental Guidance

In general, do not use DNS services on a control system. Host-based name resolution solutions are best practice. A resolving or caching DNS server is an example of a control system resource that provides name/address resolution service for local clients and authoritative DNS servers are examples of authoritative sources.

2.8.23.3 Requirement Enhancements

The control system resource that implements DNS services performs data origin authentication and data integrity verification on all resolution responses whether or not local DNS clients (i.e., stub resolvers) explicitly request this function.

2.8.24 Fail in Known State

2.8.24.1 Requirement

The control system fails to a known state for defined failures.

2.8.24.2 Supplemental Guidance

Failure in a known state can be interpreted by organizations in the context of safety or security in accordance with the organization's mission/business/operational needs. Failure in a known secure state helps prevent a loss of confidentiality, integrity, or availability in the event of a failure of the control system or a component of the system. Failure in a known safe state helps prevent systems from failing to a state that may cause injury to individuals or destruction to property.

2.8.24.3 Requirement Enhancements

The control system preserves defined system state information in failure.

2.8.25 Thin Nodes

2.8.25.1 Requirement

The control system employs processing components that have minimal functionality and data storage.

2.8.25.2 Supplemental Guidance

The deployment of control system components with minimal functionality (e.g., diskless nodes and thin client technologies) reduces the number of endpoints to be secured and may reduce the exposure of information, control systems, and services to a successful attack.

2.8.25.3 Requirement Enhancements

None.

2.8.26 Honeypots

2.8.26.1 Requirement

The control system includes components specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting, analyzing, and tracking such attacks.

2.8.26.2 Supplemental Guidance

None.

2.8.26.3 Requirement Enhancements

The control system includes components that proactively seek to identify web-based malicious code.

2.8.27 Operating System-Independent Applications

2.8.27.1 Requirement

The control system includes organization-defined applications that are independent of the operating system.

2.8.27.2 Supplemental Guidance

Operating system-independent applications are applications that can run on multiple operating systems. Such applications promote portability and reconstitution on different platform architectures, thus increasing the availability for critical functionality while an organization is under an attack exploiting vulnerabilities in a given operating system.

2.8.27.3 Requirement Enhancements

None.

2.8.28 Confidentiality of Information at Rest

2.8.28.1 Requirement

The control system protects the confidentiality of information at rest.

2.8.28.2 Supplemental Guidance

This control is intended to address the confidentiality of information in nonmobile devices.

2.8.28.3 Requirement Enhancements

The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information at rest unless otherwise protected by alternative physical measures.

2.8.29 Heterogeneity

2.8.29.1 Requirement

The organization employs diverse technologies in the implementation of the control system.

2.8.29.2 Supplemental Guidance

Increasing the diversity of technologies within the control system reduces the impact from the exploitation of a specific technology.

2.8.29.3 Requirement Enhancements

None.

2.8.30 Virtualization Techniques

2.8.30.1 Requirement

The organization employs virtualization techniques to present gateway components into control systems environments as other types of components, or components with differing configurations.

2.8.30.2 Supplemental Guidance

Virtualization techniques provide organizations with the ability to disguise gateway components into control systems environments, potentially reducing the likelihood of successful attacks without the cost of having multiple platforms.

2.8.30.3 Requirement Enhancements

1. The organization employs virtualization techniques to deploy a diversity of operating systems environments and applications.

2. The organization changes the diversity of operating systems and applications on an organization-defined frequency.

3. The organization employs randomness in the implementation of the virtualization.

2.8.31 Covert Channel Analysis

2.8.31.1 Requirement

The organization requires that control system developers/integrators perform covert channel analysis to identify those aspects of system communication that are potential avenues for covert storage and timing channels.

2.8.31.2 Supplemental Guidance

Control system developers/integrators are in the best position to identify potential avenues within the system that might lead to covert channels. Covert channel analysis is a meaningful activity when the potential exists for unauthorized information flows across security domains in the case of control systems containing export controlled information and having connections to the Internet.

2.8.31.3 Requirement Enhancements

The organization tests a subset of the vendor identified covert channel avenues to determine if they are exploitable.

2.9 Information and Document Management

Information and document management is generally a part of the company records retention and document management system. Digital and hardcopy information associated with the development and execution of a control system is important and sensitive and needs to be managed. Control system design, operations data and procedures, risk analyses, business impact studies, risk tolerance profiles, etc., contain sensitive company information and needs to be protected. Security measures, philosophy, and implementation strategies are other examples. In addition, business conditions change and require updated analyses and studies. Care is given to protect this information and verify that the appropriate versions are retained. Inherent in this is an information classification system that allows information assets to receive the appropriate level of protection.

The following are the controls for Information and Document Management that need to be supported and implemented by the organization to protect the control system.

2.9.1 Information and Document Management Policy and Procedures

2.9.1.1 Requirement

The organization develops, disseminates, and periodically reviews and updates:

1. A formal, documented, control system information and document management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance

2. Formal, documented procedures to facilitate the implementation of the control system information and document management policy and associated system maintenance controls.

2.9.1.2 Supplemental Guidance

The organization ensures the control system information and document management policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The control system information and document management policy can be included as part of the general information security policy for the organization. System information and document