13 Access Control

The "Access Control" clause is the second largest clause, containing 25 controls and 7 control objectives. This clause contains critical controls because authorized access to information processing facilities, logical or physical, is proven to be a key element in the security of these systems and applications. Organizations should place special emphasis on developing policy on many of these critical controls to set the expectation and requirements for all users—internal and external.

BUSINESS REQUIREMENTS FOR ACCESS CONTROL

Information is a business commodity and it should be protected and controlled. A series of access-related controls should be developed and implemented by management, ranging from policies, guidelines, and processes to actual safeguards that control access to information and data.

11.1.1 — Access control policy

Scope: Management should develop and publish an access control policy meeting organizational requirements including legal, regulatory, contractual, and any other special case as appropriate.
Key Risk Indicator: Yes
Control Class: (M) Management, (O) Operations
Key Questions:

- Has management developed and published a written access control policy? If so, when, and what is the scope of the policy?
- Do access control procedures and policies exist to support the access control policy?
- How frequently are access controls reviewed and by whom?
- What is the process for developing access controls?
- Is there a formal procedure for removing access rights for a terminated employee, consultant, contractor, or authorized third party? If so, please describe.

Additional Information: Access control is a key concept in information security, and organizations should take a very close look at their operations and compare their current environment against the controls in this objective to find areas for further improvement.

AU7087_C013.fm Page 174 Friday, April 28, 2006 9:45 AM

USER ACCESS MANAGEMENT

Users of the organization's information processing facilities should be authenticated and authorized in accordance with a formal policy and method. The method should take the information classification guideline into consideration and take the least-privilege approach when granting rights and permissions.

11.2.1 — User registration

Scope: Management should develop a clear set of procedures driven by policy to create and delete users from their information processing systems and applications.
Key Risk Indicator: Yes
Control Class: (M) Management, (O) Operations, (T) Technical
Key Questions:

- Is there any case where unique user accounts are not required within your information processing systems or applications?
- Does the organization have written procedures for the creation (registration) and deletion (deregistration) of user accounts?
- How is the level of access for each user account determined?
- Are users required to sign access agreements?
- Is the HR department involved in the registration and deregistration process? If so, how?
- Does management provide users with a written statement of their access rights on the organization's information processing systems?

Additional Information: Organizations should consider developing and implementing a role-based account system based on job function to help maximize time and resources required to properly implement this series of controls.

11.2.2 — Privilege management

Scope: Once a valid user account is created to access the information processing systems, privileges should be restricted and controlled in accordance with published policy and guidelines.
Key Risk Indicator: No
Control Class: (O) Operations, (T) Technical
Key Questions:

- How does your organization control privilege management for information systems and applications?
- What types of records or logs are maintained for privilege allocation?
- How are privileges granted within your organization?

Additional Information: The concept of privilege is important to information security because it is based on trust.

AU7087_C013.fm Page 175 Friday, April 28, 2006 9:45 AM

11.2.3 — User password management

Scope: Password management is an important component in controlling and managing access to information processing facilities. A formal policy and set of procedures should be developed and implemented for user password management.
Key Risk Indicator: No
Control Class: (M) Management, (O) Operations, (T) Technical
Key Questions:

- What type of management process does your organization have for passwords?
- Are users required to sign an agreement to keep their passwords confidential and private from all others?
- When a new account is created, is the user required to change his or her password to a new password conforming to company policy? If so, what is the company policy on password assignment?
- Are default password for systems, devices, or applications allowed anywhere in your information processing facilities? If so, under what circumstances?
- If the IT administration staff has to reset a user's password, what type of validation checks are performed before resetting the password?

11.2.4 — Review of user access rights

Scope: Access rights should be reviewed on a regular basis by qualified staff not responsible for account creation to ensure that the rights are in alignment with roles and responsibilities.
Key Risk Indicator: No
Control Class: (M) Management, (O) Operations
Key Questions:

- How frequently are user access rights reviewed?
- Is a formal process or method used to review user access rights? If so, please describe.
- Do you review accounts with additional privilege more frequently?
- When modifications are made to privileged accounts, how is this process carried out and is the modification maintained in a log?

USER RESPONSIBILITIES

People can be one of the best lines of defense in information security. Authorized users should be aware and trained in their responsibilities to help prevent unauthorized user access leading to an undesirable event.

AU7087_C013.fm Page 176 Friday, April 28, 2006 9:45 AM

11.3.1 — Password use

Scope: The organization's password structure should be the result of company policy based on good password practices. Users should not be allowed to override the policy.
Key Risk Indicator: No
Control Class: (M) Management, (O) Operations, (T) Technical
Key Questions:

- Does the organization require users to keep their passwords confidential? If so, how is this accomplished?
- Describe the organization's password policy (length, special characters, reuse, etc.).
- How frequently are users forced to change their passwords?

11.3.2 — Unattended user equipment

Scope: When systems and application are left unattended, management should develop controls to ensure that the unattended equipment is appropriately secured and protected.
Key Risk Indicator: No
Control Class: (O) Operations, (T) Technical
Key Questions:

- How does the organization make users aware of the security risks that arise when they leave their systems or devices unattended when logged in?
- Does the organization have any type of system override to automatically lock the system after a period of inactivity? If so, please describe.

11.3.3 — Clear desk and clear screen policy

Scope: When people are away from their work area for an extended amount of time (overnight, out for meetings, etc.), their work area should be secured and no sensitive information should be accessible in any form (paper, electronic, etc.).
Key Risk Indicator: No
Control Class: (M) Management, (O) Operations
Key Questions:

- Has the organization published a clear desk and clear screen information security policy? If so, what is the scope?
- Does management audit or monitor the operating facilities for compliance with the clear desk and clear screen policy?

NETWORK ACCESS CONTROL

Network services provide critical and trusted services for the organization. Special care should be taken to prevent unauthorized access to networked services.

AU7087_C013.fm Page 177 Friday, April 28, 2006 9:45 AM

11.4.1 — Policy on use of network services

Scope: Management should develop and create a written policy informing users that they should use only the network services they have been specifically granted.
Key Risk Indicator: No
Control Class: (O) Operations, (T) Technical
Key Questions:

- Has management developed and published a written policy on the use of network services? If so, what is the scope of the policy?
- What type of authorization is required to access the network or network services?
- If a new network connection is established at the organization's facilities, what process is required to activate the network connection?

Additional Information: Network connections and particularly Internet and wireless connections have the ability to introduce significant and unidentified risks in the environment. Management should develop a clear policy on the use and creation of networks and routinely monitor the environment to ensure that no new networks have been implemented without management approval.

11.4.2 — User authentication for external connections

Scope: A secure form of authentication should be used to control external network connections to the information processing facility.
Key Risk Indicator: No
Control Class: (O) Operations, (T) Technical
Key Questions:

- How does your organization control access and authentication of remote network connections to the information processing facilities?
- Does your organization allow VPN, dial-up, or broadband access to the information processing environment?

11.4.3 — Equipment identification in networks

Scope: As appropriate, equipment can be a secure means to authenticate network communications from a specific controlled environment and piece of equipment.
Key Risk Indicator: No
Control Class: (T) Technical
Key Questions:

- Does your organization authenticate any remote network devices based on location or equipment? If so, how is this accomplished and were all other methods determined to be inappropriate?
- If remote authentication is allowed based on location, is the remote location properly secured physically and logically?

AU7087_C013.fm Page 178 Friday, April 28, 2006 9:45 AM

11.4.4 — Remote diagnostic and configuration port protection

Scope: Diagnostic and remote ports to networking and telecommunications equipment should be closely controlled and protected from unauthorized access.
Key Risk Indicator: No
Control Class: (O) Operations, (T) Technical
Key Questions:

- Does your organization allow the use of remote diagnostic ports? If so, are external vendors or third parties allowed to access the system via the remote ports?
- Does your organization use modems for remote port connection? If so, please describe the process for modem use.
- For equipment with diagnostic or remote port management installed by default, how does your organization manage this risk?

11.4.5 — Segregation in networks

Scope: Services on the network should be segregated in logical networks when possible to increase the depth of controls.
Key Risk Indicator: Yes
Control Class: (O) Operations, (T) Technical
Key Questions:

- How does your organization segregate Internet services from the internal network?
- Does your organization allow wireless networking? If so, is wireless network traffic segregated in any way? If so, describe how.
- Does your organization require segregation in network services? If so, under what circumstances?
- Has management published a written policy on segregation of network services and associated procedures or guidelines?

Additional Information: Network services are simply network-based services such as Internet services, internal networking, wireless networking, IP telephony, video broadcasting, etc.

11.4.6 — Network connection control

Scope: When networks extend beyond organizational boundaries, special care should be taken to implement safeguards and controls to limit user connectivity and access to the network.
Key Risk Indicator: No
Control Class: (O) Operations, (T) Technical
Key Questions:

AU7087_C013.fm Page 179 Friday, April 28, 2006 9:45 AM

- Does your organization's network extend beyond your facilities and direct control? If so, is this section of the network required to comply with other network controls such as the access control policy, etc.?
- Specifically, what type of technical and operational controls does your organization implement for networks extending beyond the direct control of the organization?
- Has management published written guidelines or procedures for connection or interconnecting with networks beyond the direct control of the organization?

Additional Information: Controlling network connections to third-party vendors or external business partners can be challenging from an information security perspective and is often overlooked because they may be considered trusted network connections.

11.4.7 — Network routing control

Scope: Logical control of network routes can be critical to control the flow of data and information. Network routing control should be developed in conjunction with the access control policy of specific applications and services.
Key Risk Indicator: No
Control Class: (T) Technical
Key Questions:

- Does your organization's network extend to external parties or vendors? If so, how does management control the flow of traffic to and from the external source?
- If network routing controls have been implemented, what type of logging is used and how often are the routing controls reviewed to ensure that they are operating as designed?

Additional Information: Network routing control is a highly technical subject and, typically, only a very select few individuals in the IT department possess the knowledge to design and implement this type of control. This control is a prime candidate for validation by an external subject matter expert.

OPERATING SYSTEM ACCESS CONTROL

Operating systems are the core systems in which business applications function and perform the services required to operate the business. Special care should be taken to develop the appropriate layer of controls to protect the operating systems from unauthorized access, modification, or interruption.

AU7087_C013.fm Page 180 Friday, April 28, 2006 9:45 AM

11.5.1 — Secure log-on procedures

Scope: Operating systems should be controlled and protected by secure log-on and authentication procedures.
Key Risk Indicator: No
Control Class: (O) Operations, (T) Technical
Key Questions:

- How does your organization control access to information processing facility operating systems?
- Does your organization publish a general notice message during log-on stating that the computer should only be accessed by authorized users? If so, has this notice been reviewed and approved by your legal advisers?
- What type of alert and logging is performed for access to operating systems?
- How frequently is each critical systems access log reviewed?

11.5.2 — User identification and authentication

Scope: Each user of the organization's information processing system should have his or her own unique user account, and a secure method should be used to validate the user's identity before allowing access to the system.
Key Risk Indicator: No
Control Class: (T) Technical
Key Questions:

- Does your organization require unique user accounts for each individual? If not, under what circumstances?
- For circumstances where the identity of the user requires more than a name and password, how does your organization handle this?
- What types of authentication methods are used by your organization besides passwords?

Additional Information: There are a limited number of circumstances where a group user ID is appropriate, but they should be used only after a full risk assessment has been performed.

11.5.3 — Password management system

Scope: An automated system should be used to manage passwords and ensure that the password policy is enforced.
Key Risk Indicator: No
Control Class: (T) Technical
Key Questions:

- How does your organization manage user account passwords?

AU7087_C013.fm Page 181 Friday, April 28, 2006 9:45 AM

- Does your organization have a policy for password architecture? If so, does your password management system have the ability to enforce the requirements?
- How often does your password management system require the user to enter a new password?
- Does your password management system retain a record of previous passwords to prevent the user from using the same password again? If so, what is the management's system retention policy?

Additional Information: Password management systems are generally associated with the network, but they also apply to applications and databases.

11.5.4 — Use of system utilities

Scope: Any utilities or tools that have the ability to override the control of the system should be closely controlled and monitored.
Key Risk Indicator: No
Control Class: (O) Operations, (T) Technical
Key Questions:

- Does your organization allow the installation of utilities or tools that can override system settings? If so, under what conditions?
- If system utilities are allowed, who has access and will existing monitoring and logging capture the use of these utilities and tools?
- Does the organization publish written procedures or guidelines for the use of system utilities?

11.5.5 — Session time-out

Scope: After a predetermined amount of time, operating systems and terminals should lock to prevent unauthorized access.
Key Risk Indicator: No
Control Class: (T) Technical
Key Questions:

- Does your organization require that unattended systems be locked after a predetermined amount of time? If so, what amount of time?
- If the operating system or terminal locks after a predetermined time, how is this accomplished?
- Is it possible for the user to override the automatic locking procedure?

11.5.6 — Limitation of connection time

Scope: High-risk applications should have restrictions on connection time before locking or disconnecting.
Key Risk Indicator: No

AU7087_C013.fm Page 182 Friday, April 28, 2006 9:45 AM

Control Class: (T) Technical
Key Questions:

- Does your organization require any type of special controls for time-out or disconnection for high-risk applications? If so, are procedures or guidelines provided by management?
- What policies exist for controlling high-risk applications? Do any of these policies include the concept of limitation of connection time?

APPLICATION AND INFORMATION ACCESS CONTROL

Applications have the ability to store and process sensitive and critical data and information. Controls should be developed and implemented by management to prevent unauthorized access or tampering with such data and information.

11.6.1 — Information access restriction

Scope: Information contained in business systems and applications should be protected in accordance with the organization's access control policy and any applicable business application requirements.
Key Risk Indicator: No
Control Class: (M) Management, (O) Operations, (T) Technical
Key Questions:

- Does the organization document the class and type of information by application and system? If so, when is this process performed and how frequently is it reviewed for modification?
- How is sensitive and confidential data protected from unauthorized access and tampering at the application level?
- How is application and system output controlled?

11.6.2 — Sensitive system isolation

Scope: Highly sensitive systems should be isolated, tightly controlled, and monitored. Application or system owners should provide the requirement for isolation.
Key Risk Indicator: No
Control Class: (O) Operations
Key Questions:

- Does your organization provide a method or process for application owners to request or define the need for isolated systems? If so, please describe.
- If your organization provides the means for isolated systems, what special provisions are provided by management to allow the fulfillment of isolated systems?

AU7087_C013.fm Page 183 Friday, April 28, 2006 9:45 AM

MOBILE COMPUTING AND TELEWORKING

Mobile computing users present unique risks to the organization because they operate outside of the highly controlled network. Special controls and considerations should be given to these types of users.

11.7.1 — Mobile computing and communications

Scope: Special policies and safeguards should be developed as the result of a risk assessment to protect the organization against the risks posed by mobile and remote network communications.
Key Risk Indicator: No
Control Class: (M) Management, (O) Operations, (T) Technical
Key Questions:

- Does the organization allow the use of mobile devices such as handheld computers, laptops, and mobile phones to transmit organizational data and information?
- Has the organization published written policies, procedures, and guidelines for mobile and remote computing users? If so, what is the scope of the policies?
- Does the organization allow the use of wireless networking for mobile computing users? If so, specifically what technology and operational controls have been implemented to address the known threats with this technology?

11.7.2 — Teleworking

Scope: Remote workers require access to organizational resources including internal applications and information. Specific controls and safeguards must be developed and implemented to address the vulnerabilities associated with accessing resources external to the organization.
Key Risk Indicator: Yes
Control Class: (M) Management, (O) Operations
Key Questions:

- Has management published a policy for telecommute workers or third parties? If so, what is the scope of the policy?
- Is the network session between the remote connection and your organization's network secured and encrypted? If so, provide the technical details on how the network connection is secured.
- What special training do remote or telecommute workers or third parties receive?
- Are the concept and associated risks of remote access and telecommuting included in the organization's information security awareness program?

AU7087_C013.fm Page 184 Friday, April 28, 2006 9:45 AM

SUMMARY

"Access Control" is the second largest security clause with 25 controls and 7 control objectives. This security clause is comprehensive, covering business requirements for access control (11.1), management of user access (11.2), responsibilities of users regarding access control (11.3), special considerations for network-based access control (11.4), operational controls addressing access control risks (11.5), application-level access control of information and data (11.6), and mobile and remote telecommuting access control concepts (11.7).

REFERENCES

ISO/IEC 17799:2005 Information Technology — Security Techniques — Code of Practice for Information Security Management, International Organization for Standardization, 2005.