THEME 4

Systems of informational security

Telecommunication systems department

Lecturer: assistant professor Persikov Anatoliy Valentinovich

INTERCONNECTING SYSTEMS

A **system interconnection** is defined as the direct connection of two or more information systems for sharing data and other information resources. Organizations choose to interconnect their information systems for a variety of reasons based on their organizational needs. For example, they may interconnect information systems to exchange data, collaborate on joint projects, or securely store data and backup files.

An interconnection is a direct connection between one organization's system with another system of the same or different organization through a mechanism by which they are joined (the "pipe" through which data is made available, exchanged, or passed one way only). The "pipe" may be a dedicated line that is owned by one of the organizations or is leased from a third party (e.g., Integrated Services Digital Network [ISDN], T1 or T3 line). Alternately, the systems may be connected over a public network (e.g., Internet) using a virtual private network (VPN).

INTERCONNECTING SYSTEMS

The following are examples of interconnections:

- System A is connected to System B over a subscriber line leased by System A or System B.
- System A is segmented such that System A1 is integrated with System A but is under different management control: Authorizing Official (AO).
- System B provides data transport services between System A and System C. Here, System B is engaged in two interconnections with Systems A and C.

Levels of system interconnection may vary. For example, some organizations may choose to establish a limited interconnection, whereby users are restricted to a single application or file location with rules governing access. Other organizations may establish a broader interconnection, enabling users to access multiple applications or databases. Still other organizations may establish an interconnection that permits full transparency and access across their respective enterprises.

Interconnecting information systems can expose the participating organizations to risk. If the interconnection is not properly designed, security failures could compromise the connected systems and their data. Similarly, if one of the connected systems is compromised, the interconnection could be used as a conduit to compromise the other system and its data.

MANAGING SYSTEM INTERCONNECTIONS

All federal agencies must explicitly address the subject of interconnecting information systems by establishing formal agreements that specify the technical and security requirements of the interconnection, define the responsibilities of the participating organizations, and specify the rules governing these interconnections. In addition to an A-130, Appendix III, requirement to obtain written management authority before interconnecting information systems, OMB recommends that agencies use NIST SP 800-47 to ensure compliance for connections to non-agency systems.

When organizations are properly managing interconnected systems, the added benefits include greater efficiency, centralized access to data, and greater functionality. The security controls of each of the interconnected systems should be evaluated and meet each other's requirements for implementing security controls that are appropriate for the particular interconnection. Both organizations should specify their requirements regarding the security controls to be implemented in accordance with NIST FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, and NIST SP 800-53, Recommended Security Controls for Federal Information Systems.

MANAGING SYSTEM INTERCONNECTIONS

Each system involved in interconnection should be governed by an organization's AO who has the authority to formally assume responsibility for operating a system at an acceptable level of risk. NIST SP 800-53 specifically defines information systems connections control (specified in table) that organizations are required to implement based on an information system's security categorization. Since these categorizations and guidance apply to individual systems, agencies should carefully weigh the associated risks when systems differing in configuration or security controls are interconnected.

Identifier	Title	Control
CA-3	Information System Connections	The organization authorizes all connections from the information system to other information systems outside of the accreditation boundary and regularly monitors/controls the system interconnections. Appropriate organizational officials approve information system interconnection agreements.

MANAGING SYSTEM INTERCONNECTIONS

It is critical that both organizations maintain clear lines of communication to:

- ensure that the interconnection is properly maintained and that security controls remain effective;
- facilitate effective change management activities by making it easy for both sides to notify each other about planned system changes that could affect the interconnection; and
- enable prompt notification by both sides of security incidents and system disruptions and facilitate coordinated response, if necessary.

Identifying and implementing security controls is vital in protecting the confidentiality, integrity, and availability of the connected systems and the data that is transferred between the systems. If security controls are not in place or if they are configured improperly, the process of establishing the interconnection could expose the information systems to unauthorized access. Agencies should select applicable controls from NIST SP 800-53, based on the security categorization of the systems involved in the interconnection from FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, and NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories. The security controls should be appropriately selected in consideration of the systems that will be connected and the environment in which the interconnection will operate.

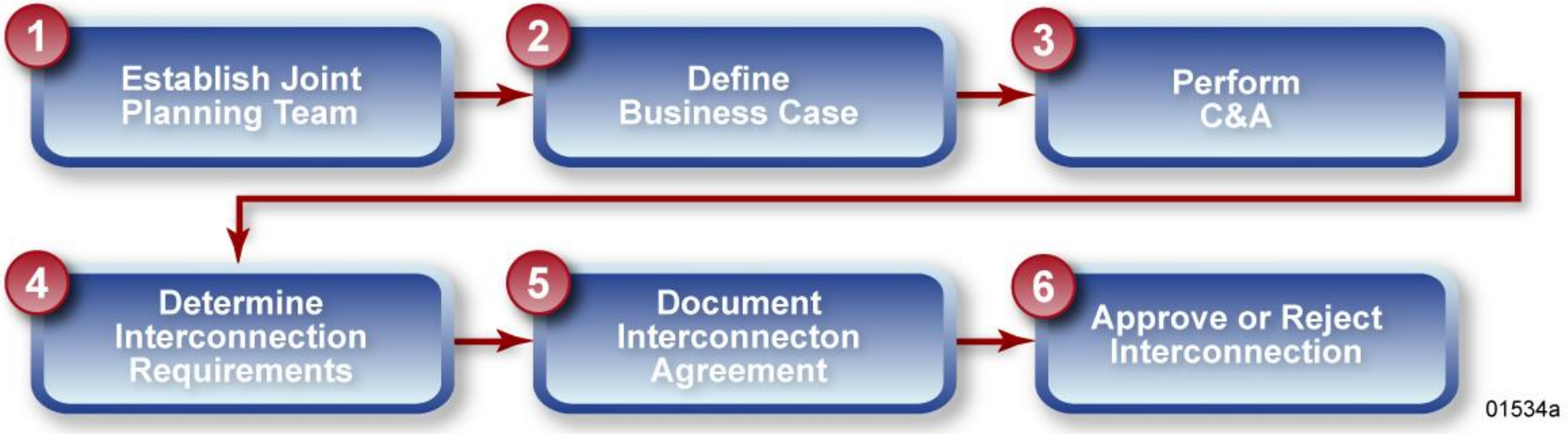
LIFE-CYCLE MANAGEMENT APPROACH

NIST SP 800-47 details a four-phase "life-cycle management" approach for interconnecting information systems that emphasizes proper attention to information security:

- **Phase 1:** Planning the Interconnection;
- **Phase 2:** Establishing the Interconnection;
- **Phase 3:** Maintaining the Interconnection; and
- **Phase 4:** Disconnecting the Interconnection.

PHASE 1: PLANNING THE INTERCONNECTION

The process of connecting two or more information systems begins with a planning phase, where the participating organizations perform preliminary activities and examine all relevant technical, security, and administrative issues. The planning phase ensures that the interconnection will operate as efficiently and securely as possible. Six steps are recommended for planning a system interconnection.



PHASE 1: PLANNING THE INTERCONNECTION

Step 1: Establish a Joint Planning Team

The organizations should consider establishing a joint planning team composed of appropriate management and technical staff that includes program managers, system security officers, system administrators, network administrators, and system architects. The typical joint planning team is responsible for coordinating all aspects of the planning process and ensuring that it has both clear direction and sufficient resources. It also must have the commitment and support of the system and data owners, and other senior managers.

Step 2: Define the Business Case

Both organizations should work together to define the purpose of the interconnection, determine how it will support their mission requirements, and identify potential costs and risks. Defining the business case will establish the basis of the interconnection and facilitate the planning process. Factors that should be considered are estimated costs (e.g., staffing, equipment, facilities), expected benefits (e.g., improved efficiency), and potential risks (e.g., technical, legal, and financial).

PHASE 1: PLANNING THE INTERCONNECTION

Step 3: Perform Certification and Accreditation

Establishing an interconnection may represent a significant change to the connected systems. Before proceeding further, each organization should consider recertification and reaccreditation of its respective system(s) to verify that security protections remain acceptable. A full security certification and accreditation might not be necessary, however, if the system continues to operate within an acceptable level of risk; in that case, an abbreviated certification and accreditation would suffice.

Step 4: Determine Interconnection Requirements

The joint planning team should identify and examine all relevant technical, security, and administrative requirements surrounding the proposed interconnection.

PHASE 1: PLANNING THE INTERCONNECTION

Step 5: Document Interconnection Agreement

The interconnection security agreement (ISA) is a security document that specifies the technical and security requirements for establishing, operating, and maintaining the interconnection. It also supports the memorandum of understanding/memorandum of agreement (MOU/MOA) between the organizations. Specifically, the ISA documents the requirements for connecting the information systems, describes the security controls that will be used to protect the systems and data, contains a topological drawing of the interconnection, and provides a signature line.

The joint planning team should document an agreement governing the interconnection and the terms under which the organizations will abide. The agreement should be based on the team's review of all relevant technical, security, and administrative requirements identified and examined in Step 4.

The MOU/MOA documents the terms and conditions for sharing data and information resources. It defines the purpose of the interconnection, identifies relevant authorities, specifies the responsibilities of each organization, defines the apportionment of costs, and identifies the timeline for terminating or reauthorizing the interconnection. In order to operate as an instrument that can be enforced by any agency that is a party to the interconnection, the MOU/MOA must be signed by an organization official, typically the authorizing official (AO).

PHASE 1: PLANNING THE INTERCONNECTION

Step 6: Approve or Reject System Interconnection

The joint planning team should submit the ISA and the MOU/MOA to the AO of each organization, requesting approval for the interconnection. Upon receipt, the AOs should review the ISA, the MOU/MOA, and any other relevant documentation or activities. Organizations may combine ISAs and MOU/MOAs to simplify their management processes and reduce paperwork if these two documents fall within the purview of the same AO. When combining ISAs and MOU/MOAs, organizations must ensure that the contents and the intent of these two documents remain unaltered.

Based on this review, the AOs should decide on one of the following:

- Approve the interconnection;
- Grant interim approval; or
- Reject the interconnection.

PHASE 2: ESTABLISHING THE INTERCONNECTION

After the system interconnection is planned and approved, it can be implemented.

PHASE 2: ESTABLISHING THE INTERCONNECTION

Step 1: Develop an Implementation Plan

To ensure that the information systems are connected properly and securely, the joint planning team should develop a system interconnection implementation plan:

- Describe the information systems that will be connected;
- Identify the sensitivity or classification level of data that will be made available, exchanged, or passed one way across the interconnection;
- Identify personnel who will establish and maintain the interconnection and specify their responsibilities;
- Identify implementation tasks and procedures;
- Identify and describe security controls that will be used to protect the confidentiality, integrity, and availability of the connected systems and data;
- Provide test procedures and measurement criteria to ensure that the interconnection operates properly and securely;
- Specify training requirements for users, including a training schedule; and
- Cite or include all relevant documentation, such as system security plans, design specifications, and standard operating procedures (SOPs).

PHASE 2: ESTABLISHING THE INTERCONNECTION

Step 2: Execute the Implementation Plan

After the implementation plan is developed, it should be reviewed and approved by senior members of the planning team and then executed. A list of recommended tasks for establishing an interconnection includes:

- Implement or configure security controls;
- Install or configure hardware and software;
- Integrate applications;
- Conduct operational and security assessments;
- Conduct security training and awareness;
- Update system security plans; and
- Perform recertification and reaccreditation.

Procedures associated with each task should be described in the implementation plan.

PHASE 2: ESTABLISHING THE INTERCONNECTION

Step 3: Activate the Interconnection

Both parties should activate the interconnection following the implementation plan execution. Each agency should closely and frequently examine the system's audit logs and the types of assistance requested by the system's users during this time to ensure that it operates properly and securely. Lastly, the appropriate agency should promptly document and address any security weaknesses or problems.

PHASE 3: MAINTAINING THE INTERCONNECTION

After the interconnection is established, the participating organizations must actively maintain it to ensure that it operates properly and securely. The following activities are recommended for maintaining the interconnection:

- Maintain the equipment;
- Manage user profiles;
- Conduct security reviews;
- Analyze audit logs;
- Report and respond to security incidents;
- Coordinate contingency planning activities;
- Perform change management; and
- Maintain system security plans.

PHASE 4: DISCONNECTING THE INTERCONNECTION

Phase-out may either be planned or it may be an emergency. Organizations may wish to restore some of the disconnections but not others.

Possibly variants include:

- terminating interconnection;
- emergency disconnection;
- restoration of interconnection;

TERMINATING INTERCONNECTION

An organization might have a variety of reasons to terminate an interconnection, for instance, changed business needs, cost considerations, or changes in system configuration. The decision to terminate the interconnection should be made by the system owner with the advice of appropriate management and technical staff. Before terminating the interconnection, the initiating party should provide written notice to the receiving party. In turn, the receiving party should acknowledge receipt of the notification. The notification should describe the reason(s) for the disconnection, provide the proposed timeline for the disconnection, and identify technical and management staff that will conduct the disconnection.

The schedule for terminating the interconnection should permit a reasonable time period for internal business planning so both sides can make appropriate arrangements. In addition, staff from both organizations should coordinate to determine the logistics of the disconnection and the disposition of shared data, including purging and overwriting sensitive data. The disconnection should be conducted when the impact on users is minimal. Following the disconnection, each organization should update its system security plan and related documents.

EMERGENCY DISCONNECTION

If one or both organizations detect an attack, intrusion attempt, or other contingency that exploits or jeopardizes the connected systems or their data, it might be necessary to abruptly terminate the interconnection without providing written notice to the other party. This extraordinary measure should be taken only in extreme circumstances and only after consultation with appropriate technical staff and senior management.

The decision to make the emergency disconnection should be made by the system owner (or a designated staff member) and implemented by technical staff. The system owner or designee should immediately notify the other party verbally and receive confirmation of the notification. Both parties should work together to isolate and investigate the incident, in accordance with incident response procedures. If necessary, law enforcement authorities should be notified, and evidence should be preserved.

The initiating party should provide a written notification to the other party in a timely manner (e.g., within five days). The notification should describe the nature of the incident, explain why and how the interconnection was terminated, and identify actions taken to isolate and investigate the incident. The notification should also specify when and under what conditions the interconnection may be restored, if appropriate.

RESTORATION OF INTERCONNECTION

Both organizations may choose to restore the system interconnection after it has been terminated. The decision to restore the interconnection should be based on the cause and duration of the disconnection. For example, if the interconnection was terminated because of an attack, intrusion, or other contingency, both parties should implement appropriate countermeasures to prevent a recurrence of the problem. If necessary, they also should modify the ISA and MOU/MOA to address issues requiring attention. Alternately, if the interconnection has been terminated for more than 90 days, each party should perform a risk assessment on its respective system and reexamine all relevant planning and implementation requirements, including developing a new ISA and MOU/MOA.

THANKS FOR ATTENTION