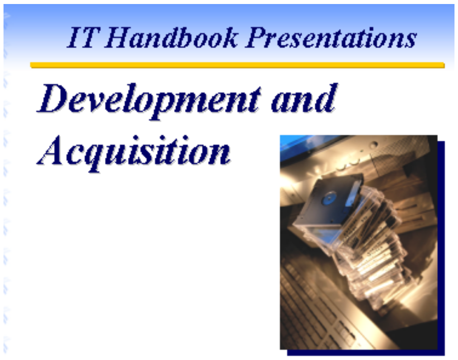
IT Examination Handbook Presentation
Development and Acquisition Booklet

Visual **Narrative**

1.



IT Handbook Presentations

Development and Acquisition

2.

Development and Acquisition

…an organization's ability to identify, acquire, install, and maintain appropriate information technology systems.

The Federal Financial Institutions Examination Council or FFIEC defines development and acquisition, or D & A as "an organization's ability to identify, acquire, install, and maintain appropriate information technology systems."

3.

Development and Acquisition

- Internal development and maintenance
- External acquisition

The process includes the internal development and maintenance of software, as well as, the acquisition of software, hardware, or services from third parties.

4.

Development and Acquisition

Federal Financial Institutions Examination Council
FFIEC
Development and Acquisition
D&A
IT EXAMINATION
HANDBOOK

- Development
- Maintenance
- Acquisition

The D & A booklet provides guidance for examiners, financial institutions and service providers regarding applications development, maintenance, and acquisition processes.

5.

Development and Acquisition

Federal Financial Institutions Examination Council
FFIEC
Development and Acquisition
D&A
IT Examination
Handbook
Federal Financial Institutions Examination Council
FFIEC
Outsourcing Technology Services
OTS
IT Examination
Handbook

The booklet does not address the acquisition of third-party services, which is addressed in the "Outsourcing Technology Services Booklet."

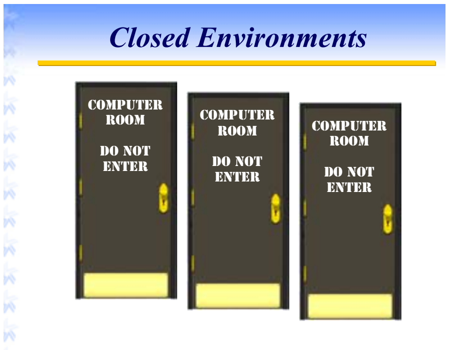
A wide variety of techniques are available to financial institutions to manage development and acquisition projects.

6.

Development and Acquisition

The structure, or formality, of project management techniques has evolved in recent years, largely in response to the increasing complexity and risks associated with modern technology systems.

7.



Closed Environments

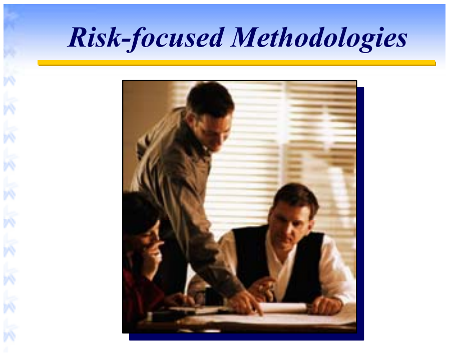
In the past, Information Technology, or IT, systems consisted of mainframes and mainframe terminals, and security could be limited to physical restrictions in these closed environments.

8.

Distributed Environments

However, modern IT systems operate in open or distributed environments that provide end users significantly increased access to systems and data.

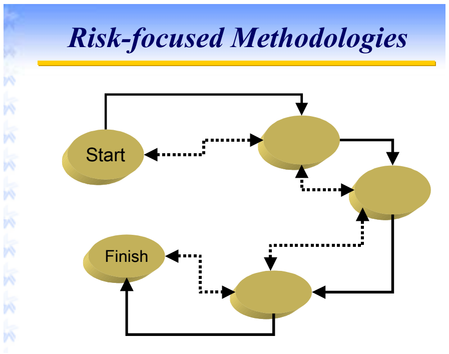
9.



Risk-focused Methodologies

The security requirements and architectural complexity of distributed IT systems have contributed to the advancement of risk-focused software development and project management methodologies.

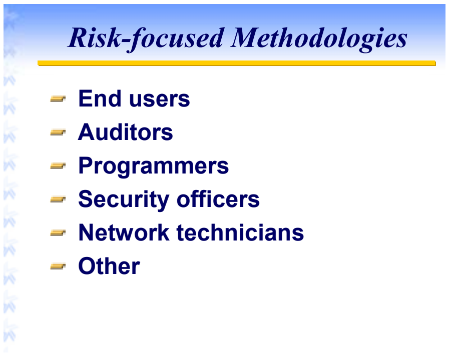
10.



Risk-focused Methodologies

The methodologies often involve iterative processes that require the repetitive, or cyclical, consideration of project risks and requirements throughout each project phase.

11.



Risk-focused Methodologies

- End users
- Auditors
- Programmers
- Security officers
- Network technicians
- Other

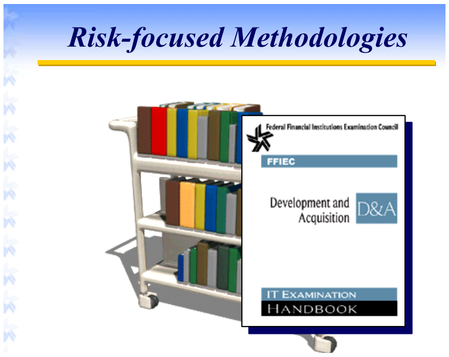
Iterative techniques help ensure the requirements of each project participant—end users, auditors, programmers, security officers, network technicians, etc.—are appropriately considered throughout a project.

12.

Risk-focused Methodologies

Many books have been written about various project management techniques and software development methodologies.

13.

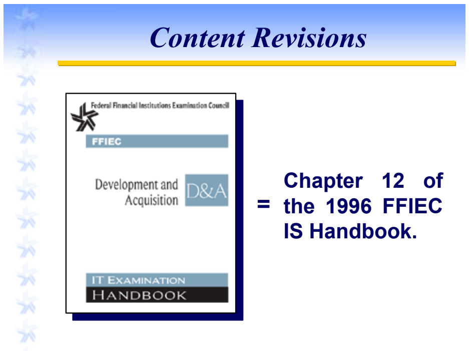


Risk-focused Methodologies

Federal Financial Institutions Examination Council
FFIEC
Development and Acquisition
D&A
IT Examination
Handbook

The D & A Booklet does not attempt to duplicate all of this information, but rather presents an overview of project management activities, risks, and risk management techniques.

14.



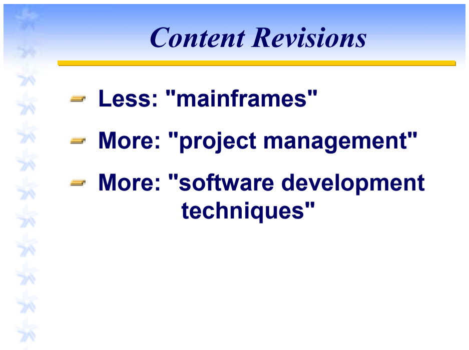
Content Revisions

Federal Financial Institutions Examination Council
FFIEC
Development and Acquisition
D&A
IT Examination
Handbook

= **Chapter 12 of the 1996 FFIEC IS Handbook.**

The D & A Booklet replaces Chapter 12 of the *1996 FFIEC IS Handbook.*

15.

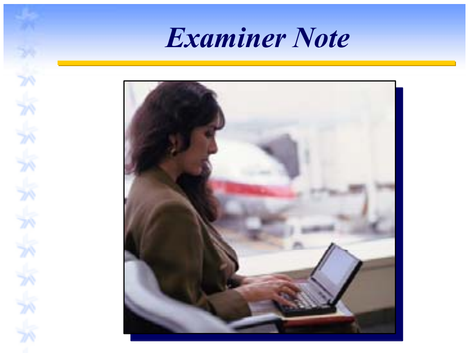


Content Revisions

- **Less: "mainframes"**
- **More: "project management"**
- **More: "software development techniques"**

The Booklet is less mainframe oriented and includes more information on project management and software development techniques.

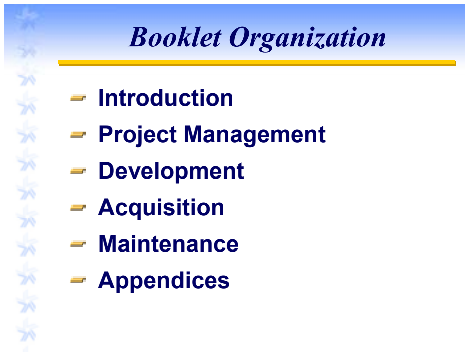
16.



Examiner Note

Financial institutions use project management techniques of varying formality and complexity. Examiners should ensure the techniques employed are appropriately matched to the complexity of a project.

17.



Booklet Organization

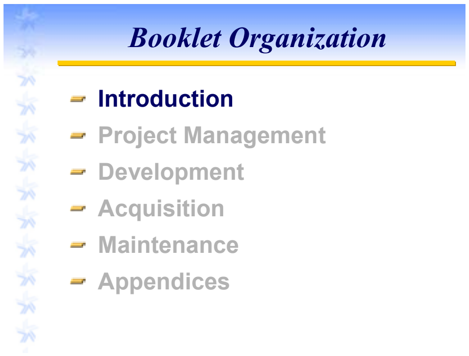
- Introduction
- Project Management
- Development
- Acquisition
- Maintenance
- Appendices

The D & A booklet is divided into six general sections:

- Introduction
- Project Management
- Development
- Acquisition
- Maintenance, and
- Appendices

Let's take a closer look at the various sections.

18.

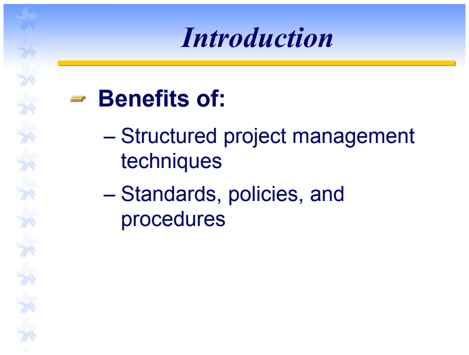


Booklet Organization

- Introduction
- Project Management
- Development
- Acquisition
- Maintenance
- Appendices

The Introduction describes development and acquisition projects and project risks, and

19.



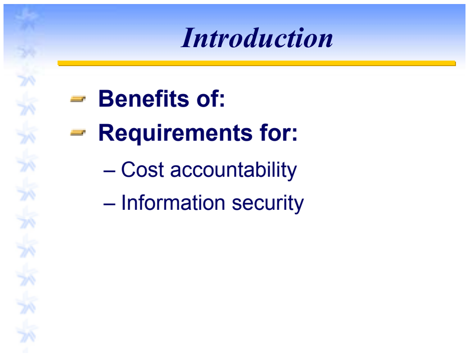
Introduction

- Benefits of:
  - Structured project management techniques
  - Standards, policies, and procedures

Points out the benefits of using:

- Structured techniques to control project activities and risks, and
- Formal project management standards, policies, and procedures.

20.



Introduction

- Benefits of:
- Requirements for:
  - Cost accountability
  - Information security

The Introduction also emphasizes the need to:

Accurately account for development and acquisition costs, and

Ensure security issues are appropriately addressed during development, acquisition, and maintenance projects.

21.

Booklet Organization

- Introduction
- Project Management
- Development
- Acquisition
- Maintenance
- Appendices

The Project Management section describes general project management considerations, including:

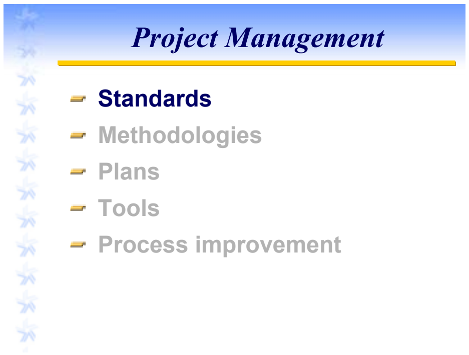
22.

Project Management

- Standards
- Methodologies
- Plans
- Tools
- Process improvement

Project management standards, methodologies, plans, tools; and methods for improving project management skills.

23.



Project Management

- Standards
- Methodologies
- Plans
- Tools
- Process improvement

Organizations should establish project management standards for all large, complex, or mission-critical projects. Institutions that routinely complete multiple projects should establish project management offices to coordinate project activities.

24.

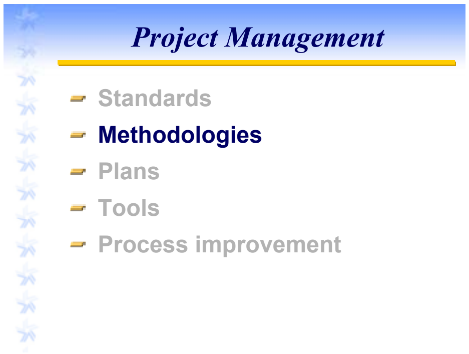
Standards

- Project plans
- Configuration management
- Quality assurance
- Risk management
- Testing
- Documentation

Organizations should develop standards for all aspects of a project, including:

- Project plans
- Configuration management
- Quality assurance
- Risk management
- Testing, and
- Documentation.

25.

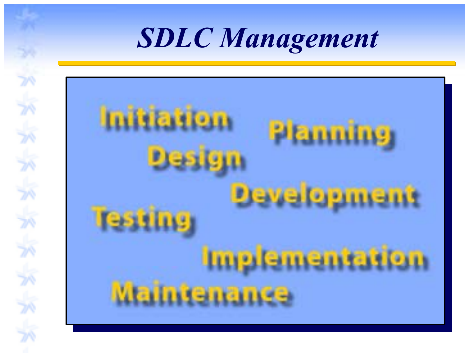


Project Management

- Standards
- **Methodologies**
- Plans
- Tools
- Process improvement

Financial institutions use various methods to manage technology projects.

26.

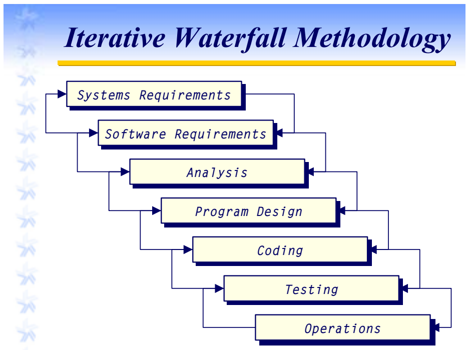


SDLC Management

Initiation
Planning
Design
Development
Testing
Implementation
Maintenance

The D & A booklet uses a systems development life cycle or SDLC model to illustrate the general project management tasks.

27.

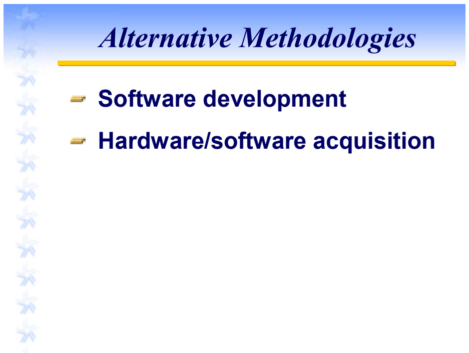


Iterative Waterfall Methodology

Systems Requirements
Software Requirements
Analysis
Program Design
Coding
Testing
Operations

The model portrayed in the booklet can be described as an iterative waterfall methodology. However, this model is offered merely as an example, and examiners should not be overly concerned with the specific terms assigned to the various project management techniques discussed in the booklet.

28.

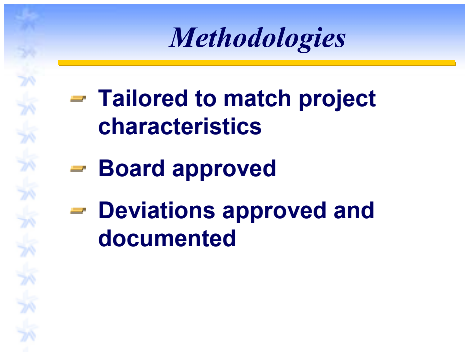


Alternative Methodologies

- Software development
- Hardware/software acquisition

Examiners should keep in mind that organizations may employ an SDLC-type technique or an alternative methodology when managing virtually any project, including: software development, and hardware, software, or service acquisition projects.

29.

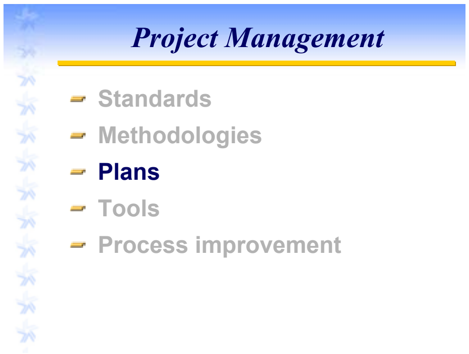


Methodologies

- Tailored to match project characteristics
- Board approved
- Deviations approved and documented

Regardless of the methodology used, it should match a project's characteristics and risks. The board, or a board-designated committee, should formally approve overall project methodologies, and management should document and approve all significant deviations from approved policies.

30.

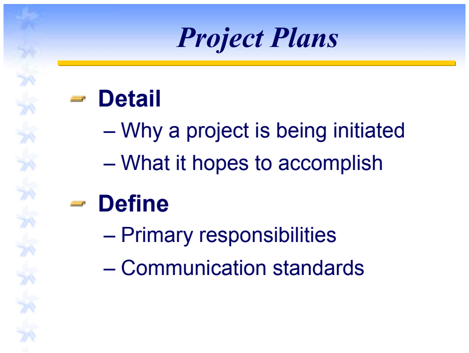


Project Management

- Standards
- Methodologies
- **Plans**
- Tools
- Process improvement

Detailed planning is one of the most critical aspects of effective project management due to the numerous interdependent issues that must be coordinated and addressed. Poor planning routinely prevents organizations from meeting project goals.

31.

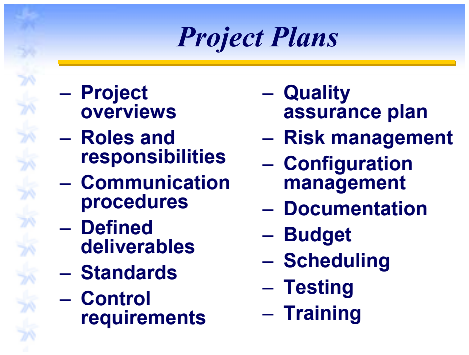


Project Plans

- Detail
  - Why a project is being initiated
  - What it hopes to accomplish
- Define
  - Primary responsibilities
  - Communication standards

Formal project plans should detail why a project is being initiated and what it hopes to accomplish. Plans should define primary responsibilities and detail the communication standards.

32.



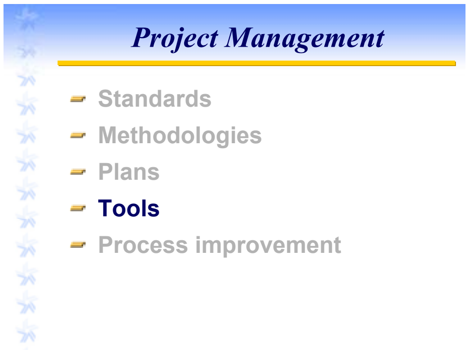
Project Plans

- Project overviews
- Roles and responsibilities
- Communication procedures
- Defined deliverables
- Standards
- Control requirements
- Quality assurance plan
- Risk management
- Configuration management
- Documentation
- Budget
- Scheduling
- Testing
- Training

Project activities should be described in as much detail as possible and include, as needed:

- A project overview
- Roles and responsibilities
- Communication procedures
- Defined deliverables
- Standards
- Control requirements
- Quality assurance plans
- Risk management
- Configuration management
- Documentation
- Budget
- Scheduling
- Testing, and
- Training

33.



Project Management

- Standards
- Methodologies
- Plans
- Tools
- Process improvement

The booklet also discusses various project management tools, such as spreadsheets or software applications, which can be used for scheduling tasks and tracking costs.

As with project methodologies, plans, and standards, the sophistication of the tools employed should match the complexity of a project.

34.

Process Improvement

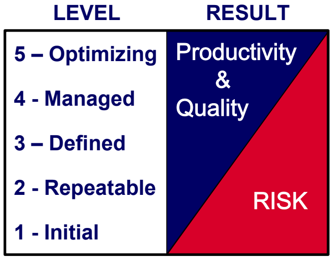
- Training
- Structured management techniques

There are several methods for enhancing the effectiveness of an organization's project management skills.

Typically the methods involve training project personnel and developing structured management techniques. For the purpose of illustration, the booklet includes two examples. These are only examples and do not constitute an endorsement of a particular brand or methodology.

35.

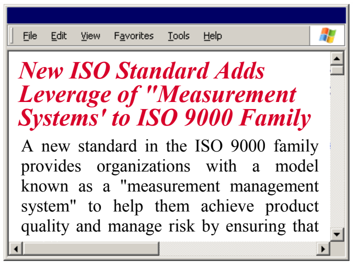
Capability Maturity Model®



The first example is the Capability Maturity Model®, developed by the Carnegie Mellon University Software Engineering Institute. This model categorizes an organization's capability to develop software into five "maturity" levels and encourages organizations to implement certain management-improvement techniques at each of these levels.

36.

International Organization for Standardization



New ISO Standard Adds Leverage of "Measurement Systems' to ISO 9000 Family

A new standard in the ISO 9000 family provides organizations with a model known as a "measurement management system" to help them achieve product quality and manage risk by ensuring that

The second example is the International Organization for Standardization or ISO's 9001 standards, which address management practices relating to design, development, production, installation, and servicing activities.

37.

9000-3 Guidelines

The generic 9001 standards focus on manufacturing activities; therefore, ISO published 9000-3 guidelines to assist project managers in applying the 9001 standards in software development environments.

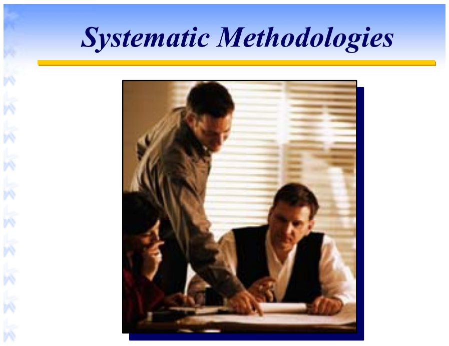
38.

Development Projects

- In-house
- Outsourcing
- Combined approach.

Development projects involve the creation of software in-house, through outsourcing, or by a combined approach.

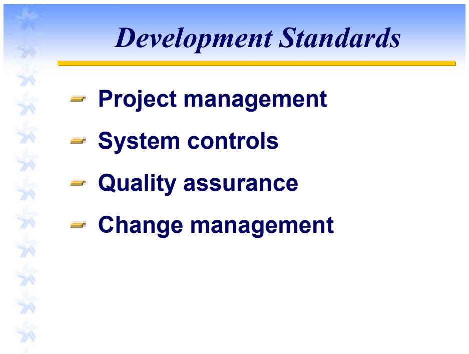
39.



Systematic Methodologies

Organizations typically manage software development projects using systematic methodologies that divide large, complex tasks into smaller, more easily managed segments or phases.

40.



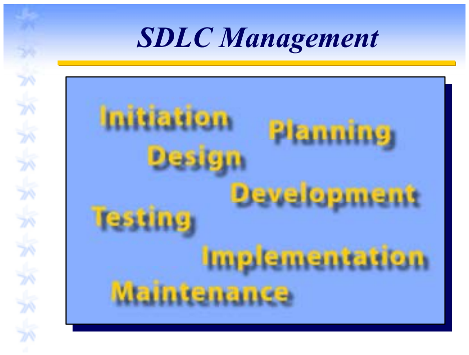
Development Standards

- Project management
- System controls
- Quality assurance
- Change management

Organizations should establish development standards that, at a minimum, address project management, system control, and quality assurance issues.

Organizations should also establish development standards that help control changes during a project.

41.



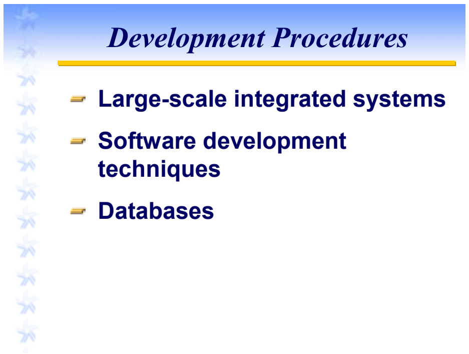
SDLC Management

Initiation
Planning
Design
Development
Testing
Implementation
Maintenance

The D & A Booklet uses the SDLC model to highlight the specific activities involved in the distinct phases of a software development project.

Various techniques can be used to complete the activities within each phase of the project. For example, prototyping is often used during initial project phases. Prototyping enhances a user's ability to visualize how systems will look and work after functional requirements are programmed.

42.



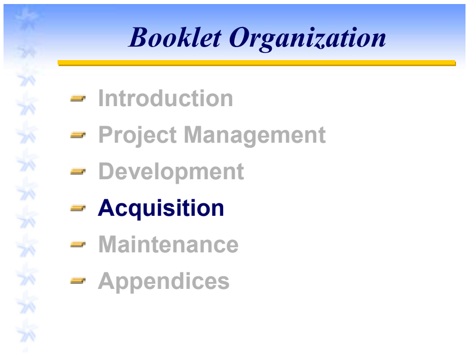
Development Procedures

- Large-scale integrated systems
- Software development techniques
- Databases

In addition, this section of the booklet looks at special requirements for:

- Large-scale integrated systems;
- Software development techniques; and
- Databases.

43.

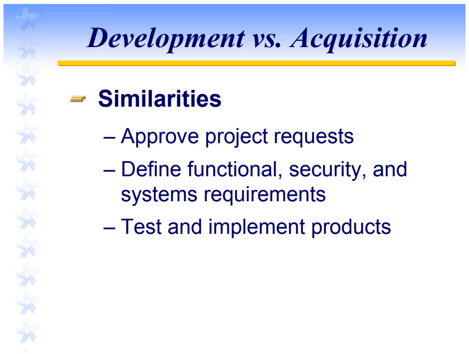


Booklet Organization

- Introduction
- Project Management
- Development
- **Acquisition**
- Maintenance
- Appendices

Acquisition projects involve many of the same activities as development projects.

44.

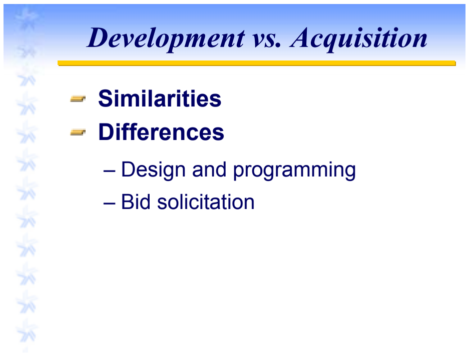


Development vs. Acquisition

- **Similarities**
  - – Approve project requests
  - – Define functional, security, and systems requirements
  - – Test and implement products

In both situations, management should approve project requests, define functional, security, and system requirements, and test and implement products.

45.

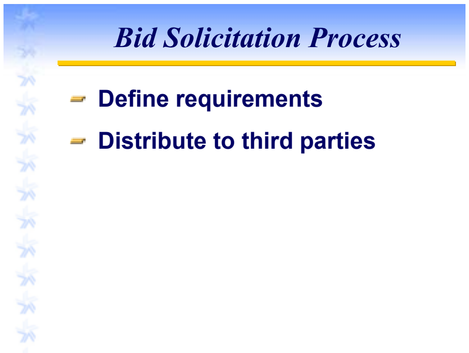


Development vs. Acquisition

- **Similarities**
- **Differences**
  - – Design and programming
  - – Bid solicitation

Differences between the two processes occur when organizations replace application design and development activities with

46.

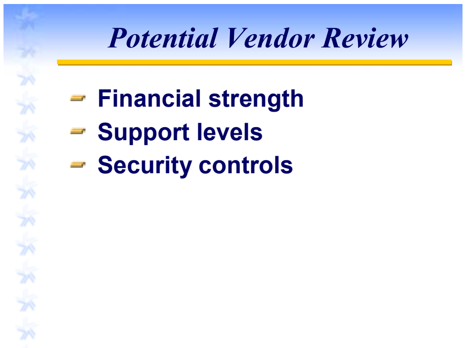


Bid Solicitation Process

- **Define requirements**
- **Distribute to third parties**

a bid solicitation process that involves developing detailed lists of functional, security, and system requirements and distributing them to third parties.

47.



Potential Vendor Review

- Financial strength
- Support levels
- Security controls

In addition to defining requirements and soliciting bids, organizations should also review potential vendors' financial strength, support levels, and security controls prior to obtaining products or services.

48.

Contract Review

Once selections are made, management should review contracts and licensing agreements to ensure the rights and responsibilities of each party are clear and equitable.

49.

Foreign-based Third Parties

Acquiring software from foreign-based third parties presents additional challenges, and organizations should appropriately manage the unique risks presented by these arrangements.

50.

Foreign-based Third Parties

For example, organizations should decide which country's laws will control the relationship and ensure that they and their vendors comply with applicable laws and regulations. More information on issues institutions need to consider when dealing with foreign entities can be found in Appendix C of the Outsourcing Technology Services booklet.

51.

Acquisition

- Escrowed source code and documentation
- Contracts and licensing agreements

The D & A booklet supplements the acquisition section with two sub sections—one on escrowing of source code and documentation and another on contracts and licensing agreements.

52.

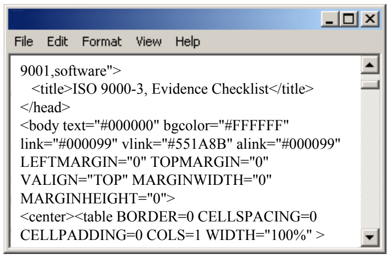
Escrow

- Allows institution to obtain source code and documentation if vendor cannot support the product
- Held by an independent third party

Typically an institution will not receive the source code when software is licensed from a vendor. In the event the vendor cannot continue to support the software, due to bankruptcy for example, the institution will need access to the source code to make any necessary changes and updates.

53.

SOURCE CODE ACCESS



```
9001,software">
   <title>ISO 9000-3, Evidence Checklist</title>
</head>
<body text="#000000" bgcolor="#FFFFFF"
link="#000099" vlink="#551A8B" alink="#000099"
LEFTMARGIN="0" TOPMARGIN="0"
VALIGN="TOP" MARGINWIDTH="0"
MARGINHEIGHT="0">
<center><table BORDER=0 CELLSPACING=0
CELLPADDING=0 COLS=1 WIDTH="100%" >
```

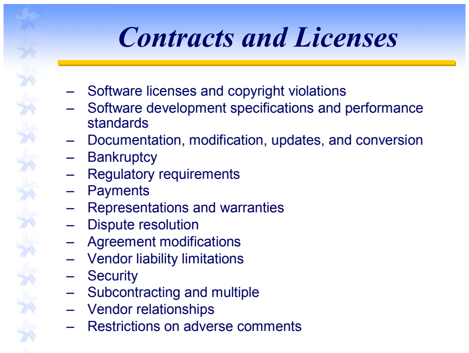
To ensure the institutions have access to the source code, the code and accompanying documentation can be put into escrow with an independent third party. Under certain circumstances, the escrow agent may be authorized to release copies to specified parties.

54.

Contracts and Licenses

All contracts between an organization and a software vendor should clearly describe the rights and responsibilities of all the parties to the contract.

55.

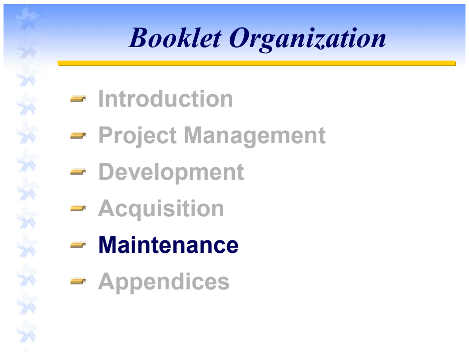


Contracts and Licenses

- Software licenses and copyright violations
- Software development specifications and performance standards
- Documentation, modification, updates, and conversion
- Bankruptcy
- Regulatory requirements
- Payments
- Representations and warranties
- Dispute resolution
- Agreement modifications
- Vendor liability limitations
- Security
- Subcontracting and multiple
- Vendor relationships
- Restrictions on adverse comments

One of the most important licensing issues is the definition used for the precise scope of the license. Organizations should ensure licenses clearly state whether software usage is exclusive or non-exclusive, how many individuals at an organization can use the software, and whether there are any location limitations on its use.

56.

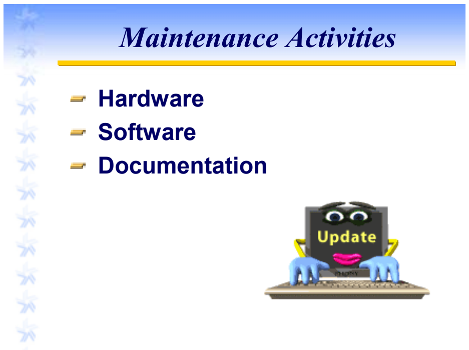


Booklet Organization

- Introduction
- Project Management
- Development
- Acquisition
- **Maintenance**
- Appendices

After an application or system is installed, it should be maintained. Often the resources required to maintain an application or system exceed those required to develop or acquire it.

57.



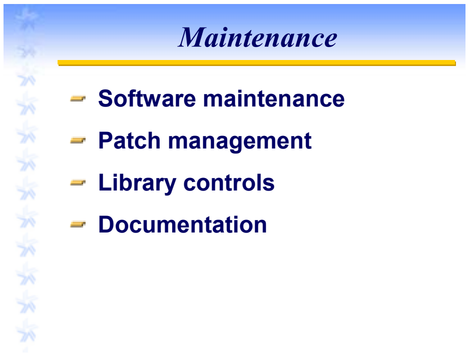
Maintenance Activities

- **Hardware**
- **Software**
- **Documentation**

Maintenance includes the routine servicing and periodic modification of hardware, software, and documentation.

- Organizations periodically upgrade or replace outdated or malfunctioning equipment to enhance security, performance, or storage.
- Software is often modified to address changed user requirements, rectify software problems, introduce new functionality, correct security vulnerabilities, or implement new technologies.
- Documentation maintenance is necessary to ensure technology related records, standards, and procedures are current and accurate.

58.



Maintenance

- **Software maintenance**
- **Patch management**
- **Library controls**
- **Documentation**

Maintenance issues addressed in the booklet include:

- Major, routine, and emergency changes,
- Software patches,
- Library controls, and
- Documentation maintenance.

59.

Booklet Organization

- Introduction
- Project Management
- Development
- Acquisition
- Maintenance
- **Appendices**

The booklet is supplemented with two appendices, Examination Procedures and a Glossary.

Examiners should carefully select procedures that will provide the most appropriate risk-focused assessment of the development and acquisition activities of the institution being examined.

60.

URSIT

Booklet: Supervision of Technology Service Providers
Section: Appendix D: Uniform Rating System for Information Technology

RATING COMPONENTS
- AUDIT
- MANAGEMENT
- DEVELOPMENT AND ACQUISITION
- SUPPORT AND DELIVERY

The workprogram parallels the risk assessment guidelines in the FFIEC Uniform Rating System for Information Technology.

61.

Workprogram

- **Checklists**
- **Development contracts**
- **Licensing agreements**

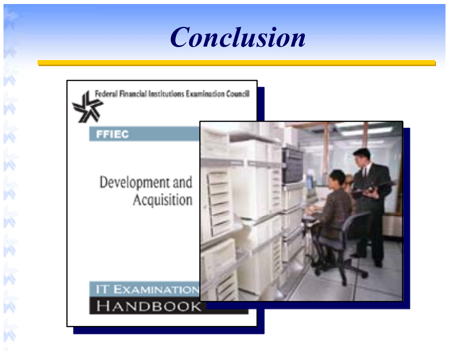
The workprogram also includes checklists for assessing other areas such as patch management, development contracts, and licensing agreements.

62.

Conclusion

Federal Financial Institutions Examination Council
FFIEC
Development and Acquisition
D&A
IT EXAMINATION
HANDBOOK

In general, examiners should find the D & A booklet provides a basic overview of industry-standard project management techniques and a solid basis for assessing project management risks.

63. 

Conclusion

Federal Financial Institutions Examination Council
FFIEC
Development and Acquisition
IT EXAMINATION
HANDBOOK

Additionally, financial institutions should find implementation of various booklet concepts enhance their ability to, "identify, acquire, install, and maintain appropriate information technology systems."