OUSD(C) Web-based Curriculum Development

Financial Improvement and Audit Readiness 301 (FIAR 301)

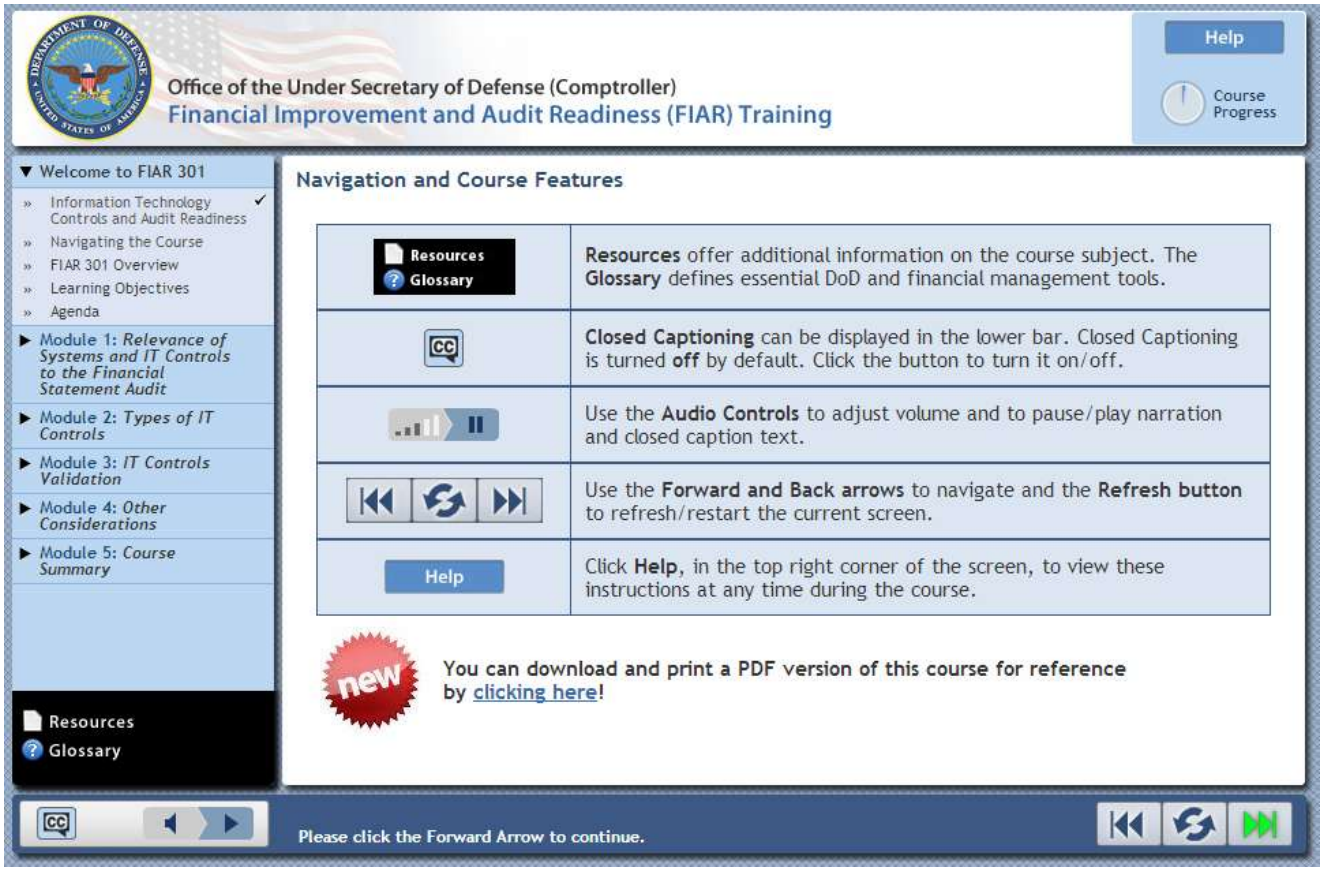
December 2012

Welcome to FIAR 301

Thank you for participating in this course – Financial Improvement and Audit Readiness – or FIAR - 301. The course, designed and developed by the Office of the Under Secretary of Defense, Comptroller, FIAR Directorate, provides an in-depth review on the importance of automated systems for audit readiness and includes an overview on the types of information technology controls and how to document and test them.

At the end of this course, you will have an opportunity to complete a survey – please let us know what worked well or what needs improvement. Your feedback at the end of this course will help us improve future versions of this and other courses in the FIAR Curriculum.

Please click the Forward arrow to continue.



Navigation and Course Features

Two important elements of this course are the Resources and Glossary of terms. Resources offer additional information on the course subject. The Glossary defines essential DoD and financial management tools used in this course. Links to both are located on the bottom of the left-hand navigation menu. Closed Captioning can be displayed in the lower bar.

Closed Captioning can be displayed in the lower bar. Closed Captioning is turned "off" by default. Click the Closed Caption button to turn it on or off based on your preference. The on/off button is located in the bottom-left menu tray.

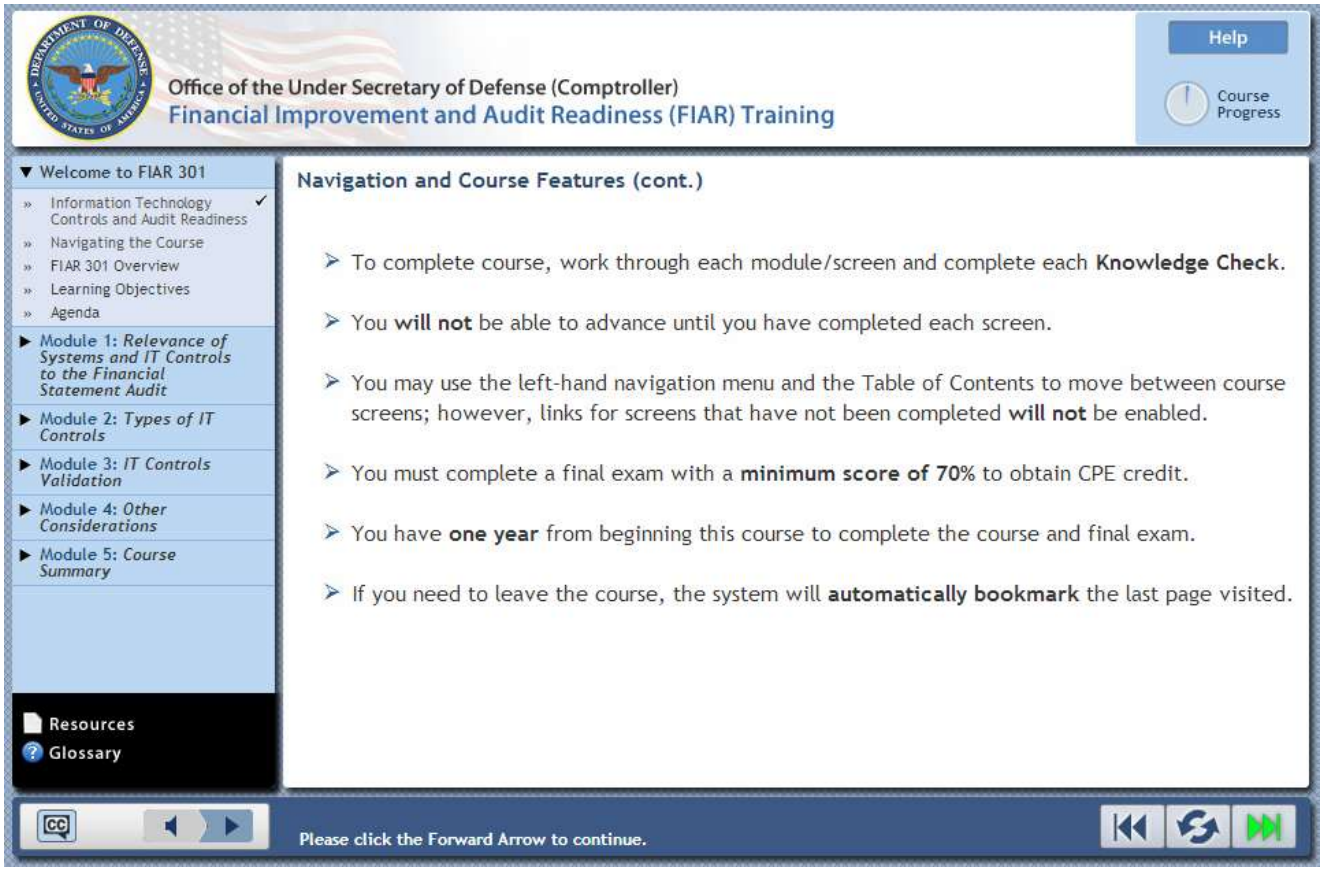
Use the Audio Controls to adjust volume and to pause or play narration and Closed Caption text. The audio controls are also located in the bottom-left menu tray.

Use the Forward and Back arrows to navigate the course screens and the Refresh button to refresh or restart a current screen. These controls are located in the bottom-right menu tray.

Click Help, in the top right corner of the screen, to view these instructions at any time during the course.

Now, you can download and print the PDF version of this course for reference by clicking on the link at the bottom of this screen. You will also be able to find the PDF version of this course in the Resources section, and may download the file at any time. There will also be a download link provided on the final screen of this course as a reminder.

Please click the Forward arrow to continue.



Navigation and Course Features (cont.)

To complete the course, please work through each module and screen, and complete each Knowledge Check.

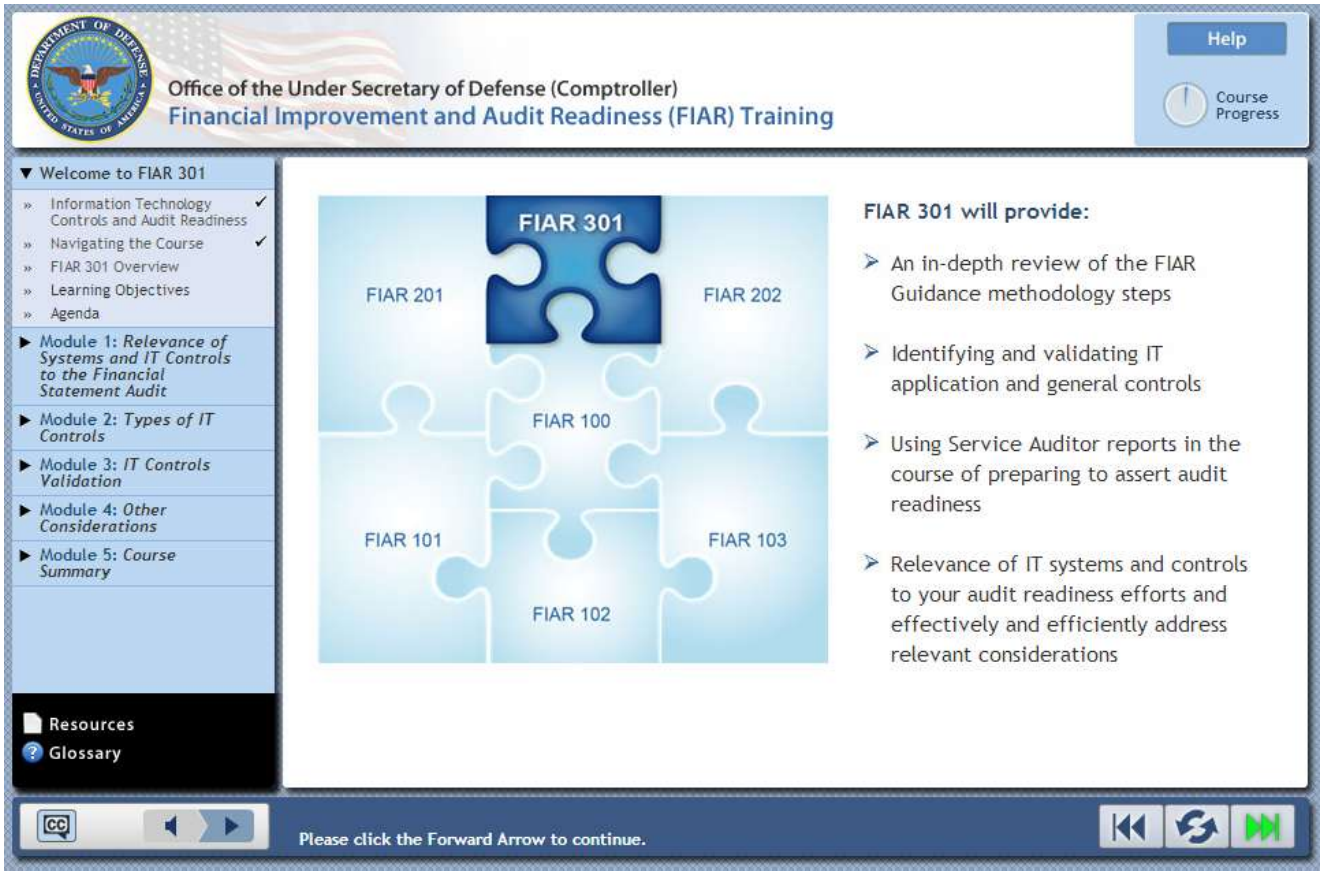
You will not be able to advance until you have completed each screen.

You may use the left-hand navigation menu and the Table of Contents to move between course screens; however, links for screens that have not been completed will not be enabled.

At the end of the course, you must complete a final exam to obtain CPE credit. A minimum score of 70% is required to receive credit. You will have up to one year from the date you begin this course to complete the course and achieve the required score on the final exam.

If you need to leave the course and cannot complete it, the system will automatically bookmark the last page visited and will send you there when you return to the course.

Please click the Forward arrow to continue.

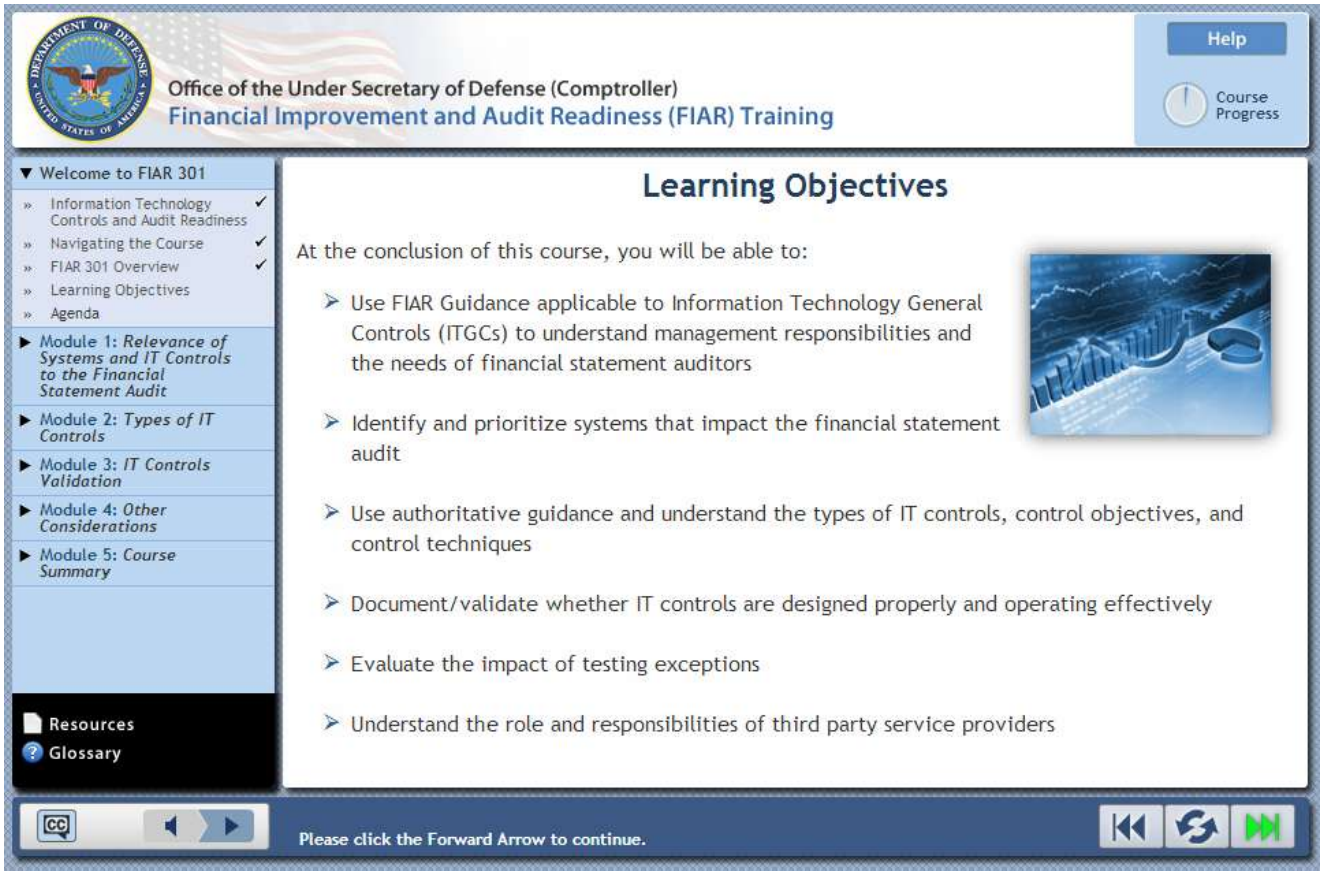


FIAR Overview

This course is part of the foundation of the FIAR Curriculum.

FIAR 301 will provide an in-depth review of the FIAR Guidance methodology steps to be followed when determining which IT systems should be considered in or out of scope for audit readiness purposes, identifying and validating IT application and general controls, and using Statement on Standards for Attestation Engagements – or SSAE - No. 16 reports in the course of preparing to assert audit readiness.

Please click the Forward arrow to continue.

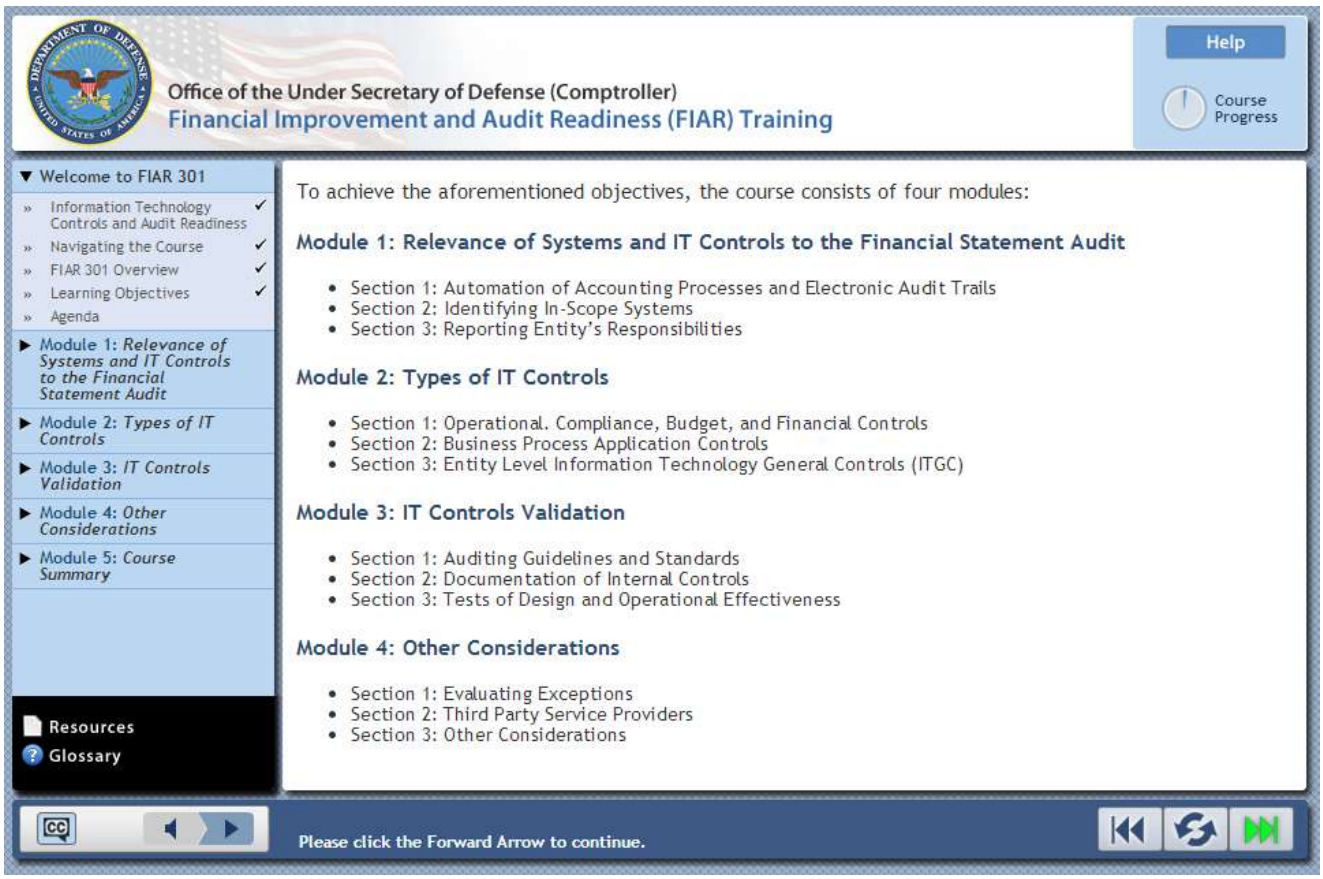


Learning Objectives

At the conclusion of this course, you will be able to:

- Use FIAR Guidance applicable to Information Technology General Controls - or ITGCs - to understand management responsibilities and the needs of financial statement auditors;
- Identify and prioritize systems that impact the financial statement audit;
- Use authoritative guidance and understand the types of information technology controls, control objectives, and control techniques;
- Document and validate whether information technology controls are designed properly and operating effectively;
- Evaluate the impact of testing exceptions; and
- Understand the role and responsibilities of third party service providers.

Please click the Forward arrow to continue.



Agenda

To achieve the aforementioned objectives, the course consists of the following four modules:

Module 1: Relevance of Systems and IT Controls to the Financial Statement Audit

Module 1 includes Section 1: Automation of Accounting Processes and Electronic Audit Trails; Section 2: Identifying In-Scope Systems; and Section 3: Reporting Entity's Responsibilities

Module 2: Types of IT Controls

Module 2 includes Section 1: Operational, Compliance, Budget, and Financial Controls; Section 2: Business Process Application Controls; and Section 3: Entity Level Information Technology General Controls

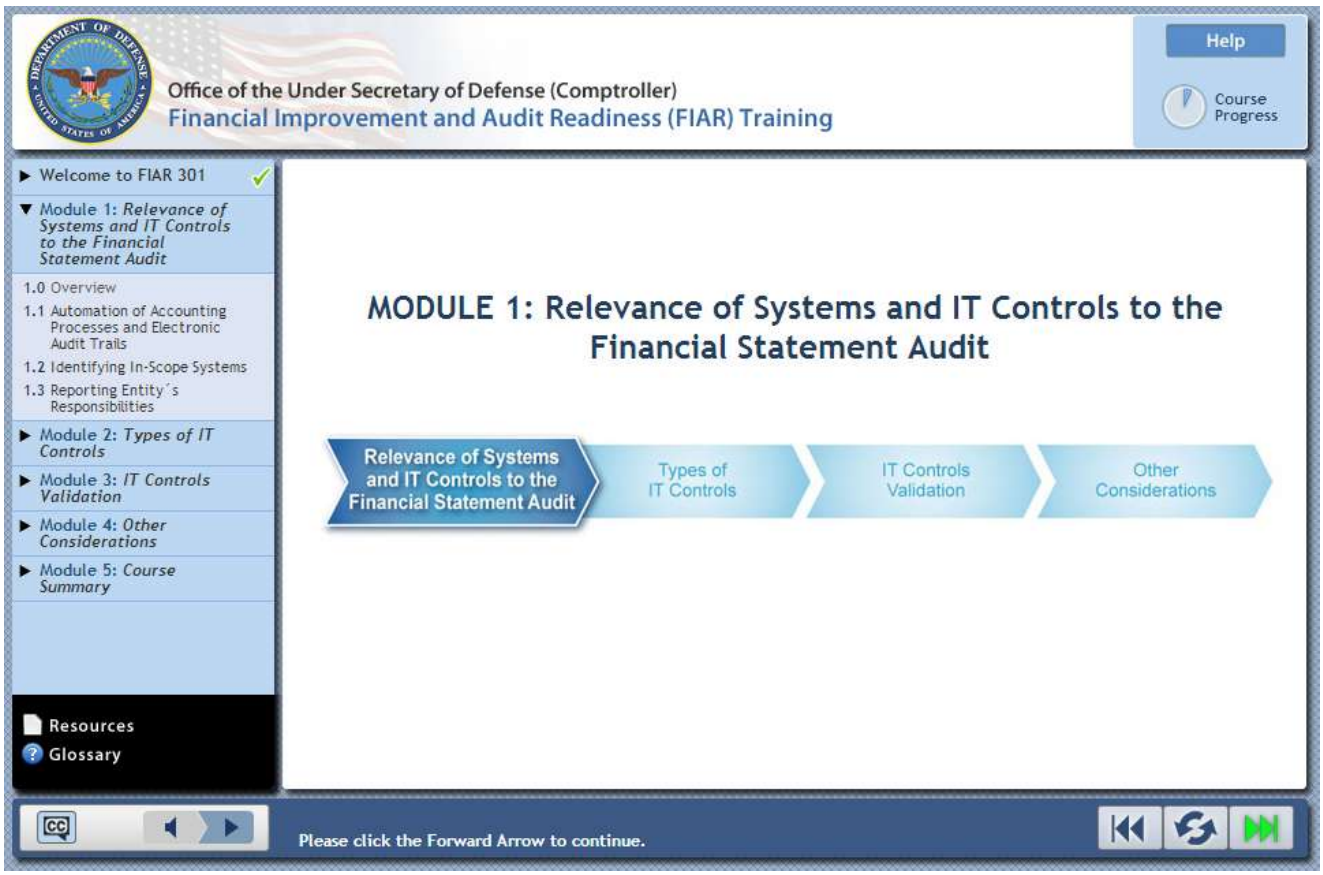
Module 3: IT Controls Validation

Module 3 includes Section 1: Auditing Guidelines and Standards; Section 2: Documentation of Internal Controls; and Section 3: Tests of Design and Operational Effectiveness

Module 4: Other Considerations:

Module 4 includes Section 1: Evaluating Exceptions; Section 2: Third Party Service Providers; Section 3: Other Considerations

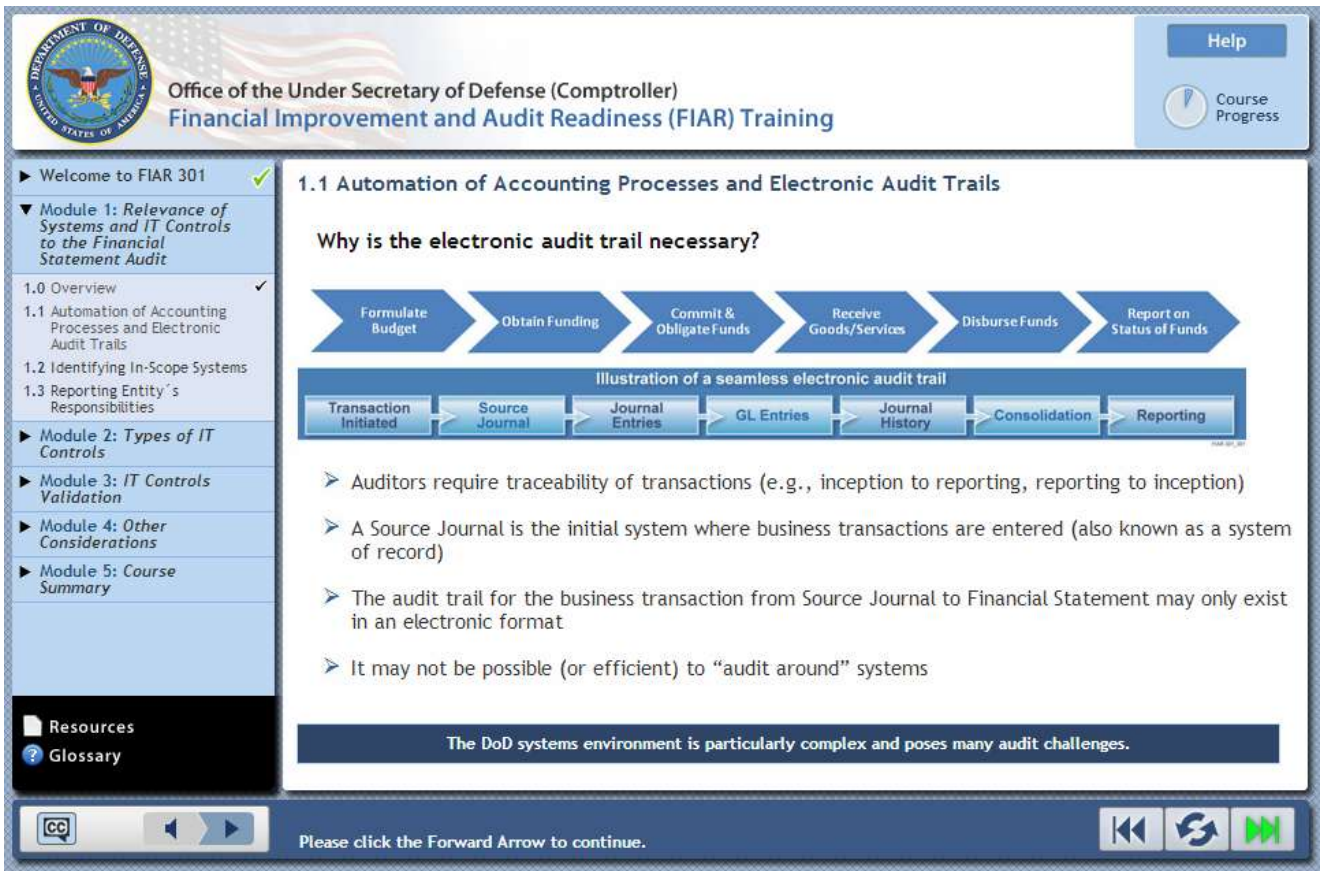
Please click the Forward arrow to continue.



Module 1 Intro: Relevance of Systems and IT Controls to the Financial Statement Audit

This module introduces the relevance of automated information systems and IT controls to the financial statement audit.

Please click the Forward arrow to continue.



1.1 Automation of Accounting Processes and Electronic Audit Trails

Today, most DoD business transactions are recorded in computerized information systems. In order to adequately audit these transactions, auditors must be able to "follow" the transaction from inception to reporting and vice versa.

A Source Journal is the initial system where business transactions are entered (also known as a system of record).

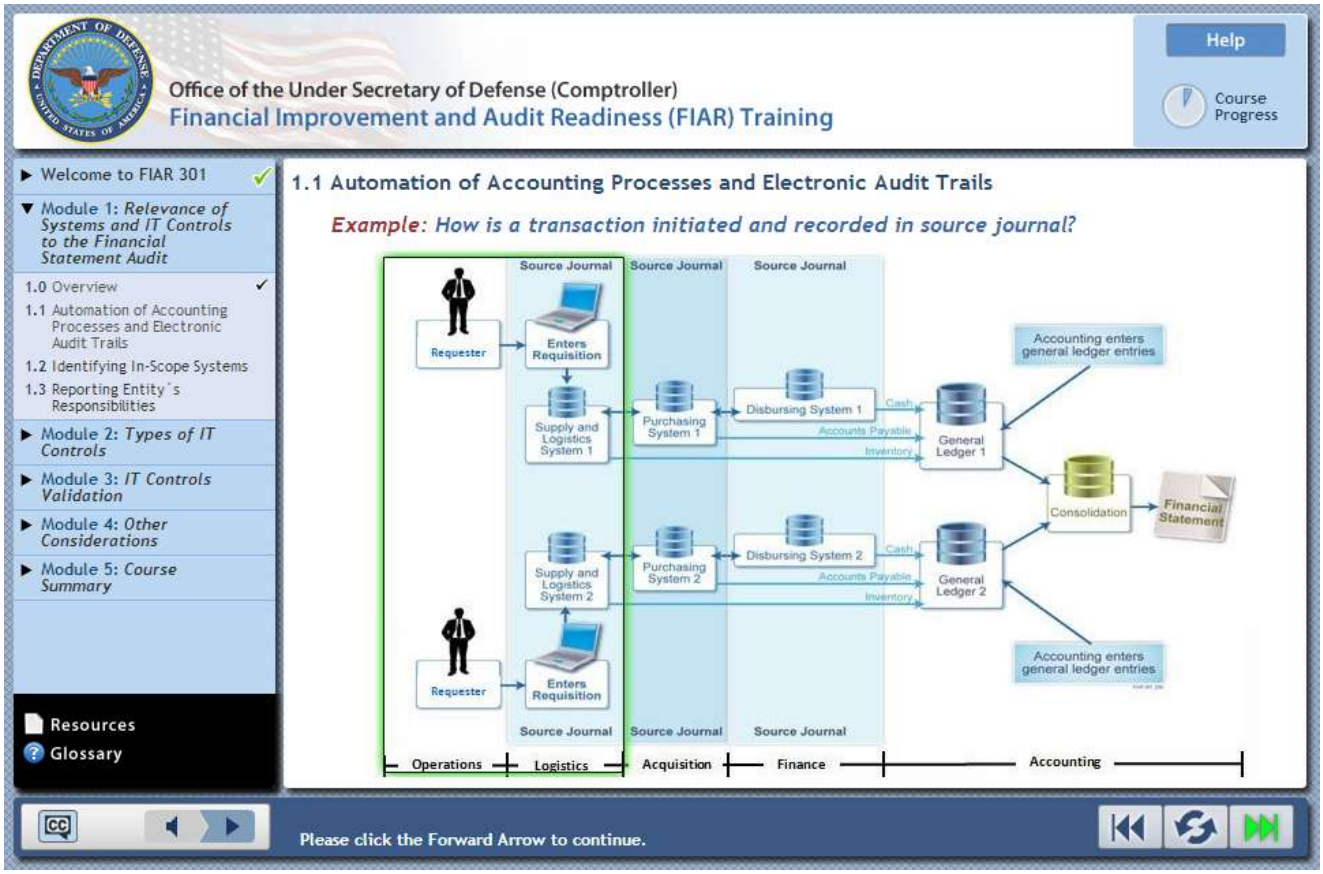
The flow of information from point of transaction initiation in source journals through posting in the general ledger and consolidation systems generally occurs electronically and with limited external supporting documentation.

Given this dependence on computerized systems, it may not be possible to "audit around" these systems as physical source documentation may not exist. Instead, a Reporting Entity may have to "audit through" these systems using ITGCs.

Even in those instances where it may be possible to "audit around" the Department's information systems, it will likely be inefficient to do so given the high volume of transactions flowing through the systems and correspondingly large sample sizes required to sufficiently audit the transactions and activity.

The DoD systems environment is particularly complex and poses many audit challenges due to the large number of legacy systems involved, the ongoing transition to Enterprise Resource Planning - or ERP - systems, and the existence of multiple system owners and other service providers.

Please click the Forward arrow to continue.



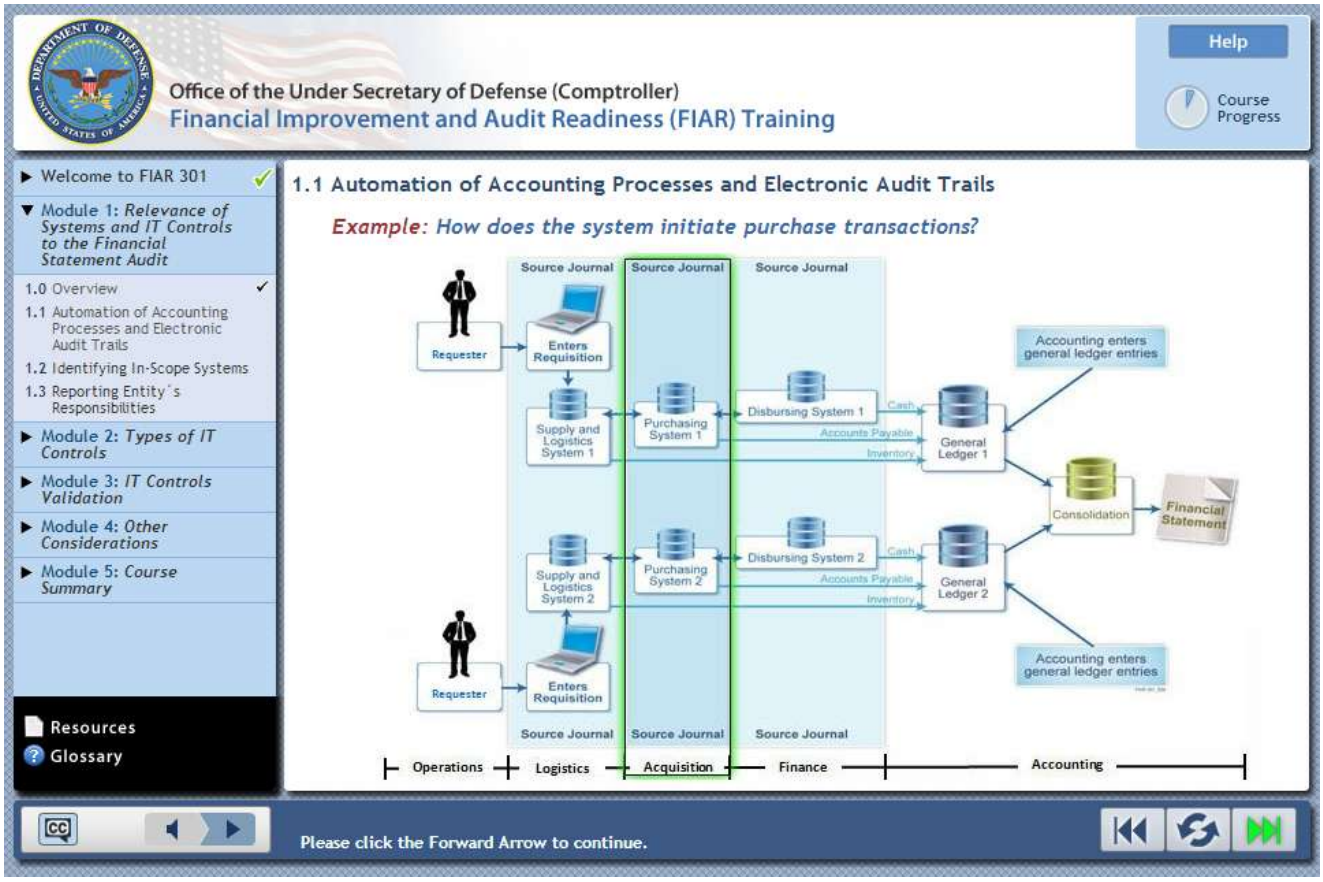
How is a transaction Initiated and recorded in source journal?

To better illustrate this concept, we have prepared a graphic which we will refer to at various points throughout this course. This example will illustrate the end-to-end flow of information generated by the requisition of material to support operations.

Our example begins when a requester prepares and electronically enters a requisition in a requisitioning system to obtain a truck needed to transport supplies and other materials to troops under their command.

The supply and logistics system electronically processes the approved requisition and provides the electronic authorization to remove an item from inventory in the supply system and the general ledger.

Please click the Forward arrow to continue.

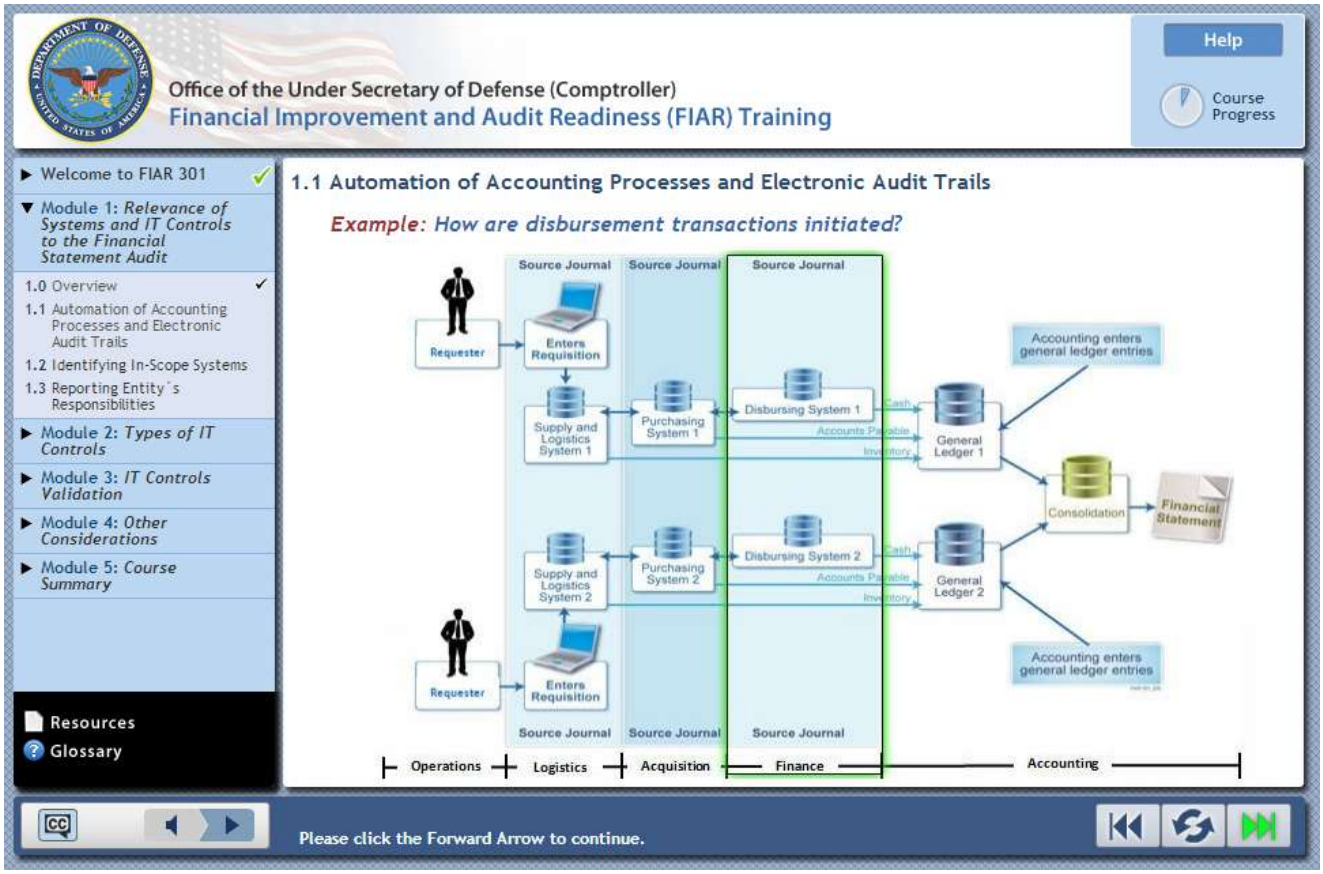


How does the system initiate purchase transactions?

If inventory levels in the supply and logistics system fall below certain predetermined levels, the system may automatically initiate a purchase requisition or order in a purchasing system if it is configured to do so and funds are available. The purchasing system may in turn provide information to the general ledger to record an obligation.

In addition, the purchasing system may initiate a purchase order when inventory level falls below predetermined levels. In this instance, there are no requesters or approvers because it is an automated process. Reporting entities need to verify that the system is configured so the system is only initiating purchase orders when those predetermined levels are reached.

Please click the Forward arrow to continue.



How are disbursement transaction initiated?

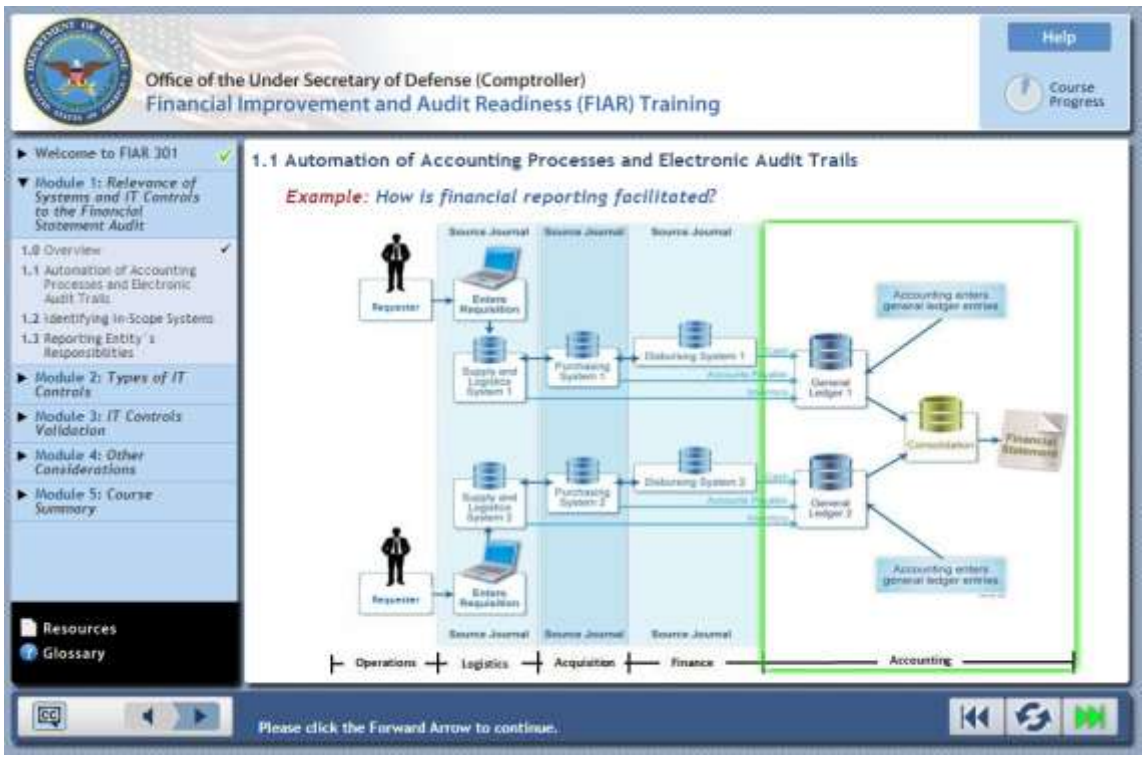
Once ordered materials have been received, they are inspected for acceptance and approval. Once approved, an accounts payable is recorded in the general ledger.

Once the vendor's invoice is received, a three way match between the vendor's invoice, original purchase order or contract, and receiving report is performed to ensure accuracy and completeness of all goods received.

Upon approval of the vendor's invoice for payment, the payment is processed through the disbursing system to liquidate the obligation. A Funds Availability check should also be performed - ideally by the system - prior to executing disbursement, since it is required by the Grassley Act. The general ledger will be updated to reflect a reduction in the accounts payable balance and a corresponding reduction in cash, or Fund Balance with Treasury.

Key supporting documents, or KSDs, to support each financial event that occurred in each step of the process – from purchase order, to receiving report, to invoice -- including control activities, will likely exist both inside and outside the information systems (such as an electronic audit trail or physical documentation, respectively).

Please click the Forward arrow to continue.



How is financial reporting facilitated?

At the end of the accounting period, information from the general ledgers are passed to a system that consolidates financial information from all DoD reporting entities - such as the Defense Departmental Reporting System (or DDRS). The information system uses the consolidated information to prepare the Department wide financial statements.

The key point we are trying to illustrate with our example extends beyond the fact that the general ledger and accompanying financial systems produce accounting data and therefore are relevant to audit readiness. We also want to emphasize that the number of systems used to record, process, summarize and report financial information introduces additional complexities and risks.

It is also important to note that while information in each of these systems is used for financial reporting, it is also used to support ongoing business operations. For example:

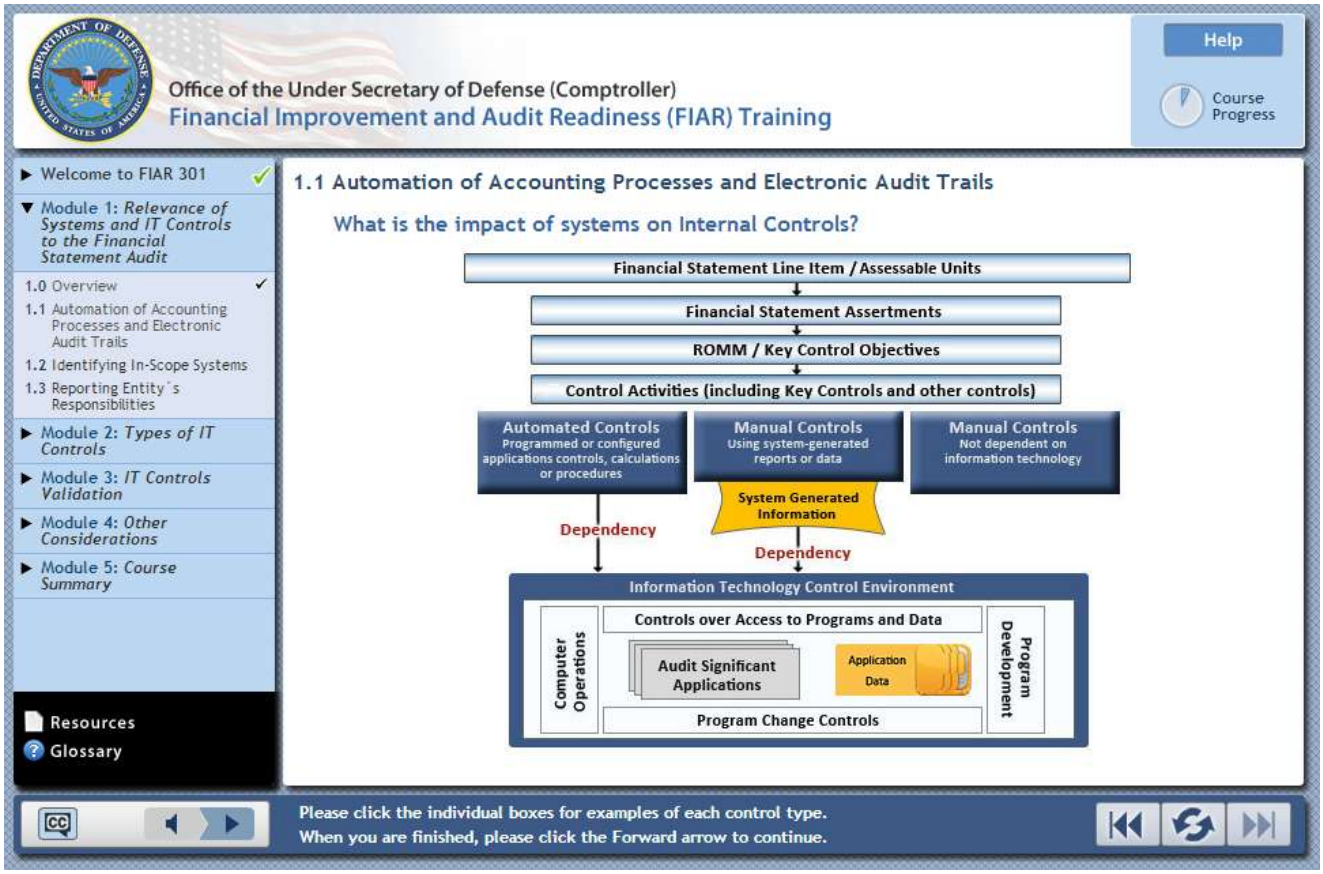
If information in the supply and logistics systems is incorrect, the combatant commander may not have visibility into resource availability or the status of requested items.

If the information is not completely and accurately transferred to the purchasing systems, needed materials and equipment may not be ordered in a timely manner and/or visibility into the availability of funds may be impaired if purchase orders and contracts are not recorded in a timely manner.

If invalid or inaccurate information is entered into disbursing systems - manually or interfaced - duplicate or erroneous payments could be made to vendors and deplete resources available to the Department, not to mention possible Anti-Deficiency Act violations that may occur if we execute payments in excess of allowable spending authority.

Now that we have an understanding of the importance of automated systems to the Department's operational and accounting processes, we would like to discuss the significance of internal controls within and around these systems to the Department's overall audit readiness efforts and associated internal controls over financial reporting.

Please click the Forward arrow to continue.



What is the impact of systems on Internal Controls?

The terms and concepts on this screen will be discussed in greater detail throughout the remainder of this course, but it is introduced here to emphasize several fundamental points:

The Reporting Entity's financial statements and individual line items, such as Outlays, are supported by one or more business processes - such as Procure to Pay or Hire to Retire - or class of transactions - such as travel, payroll or contract expenses.

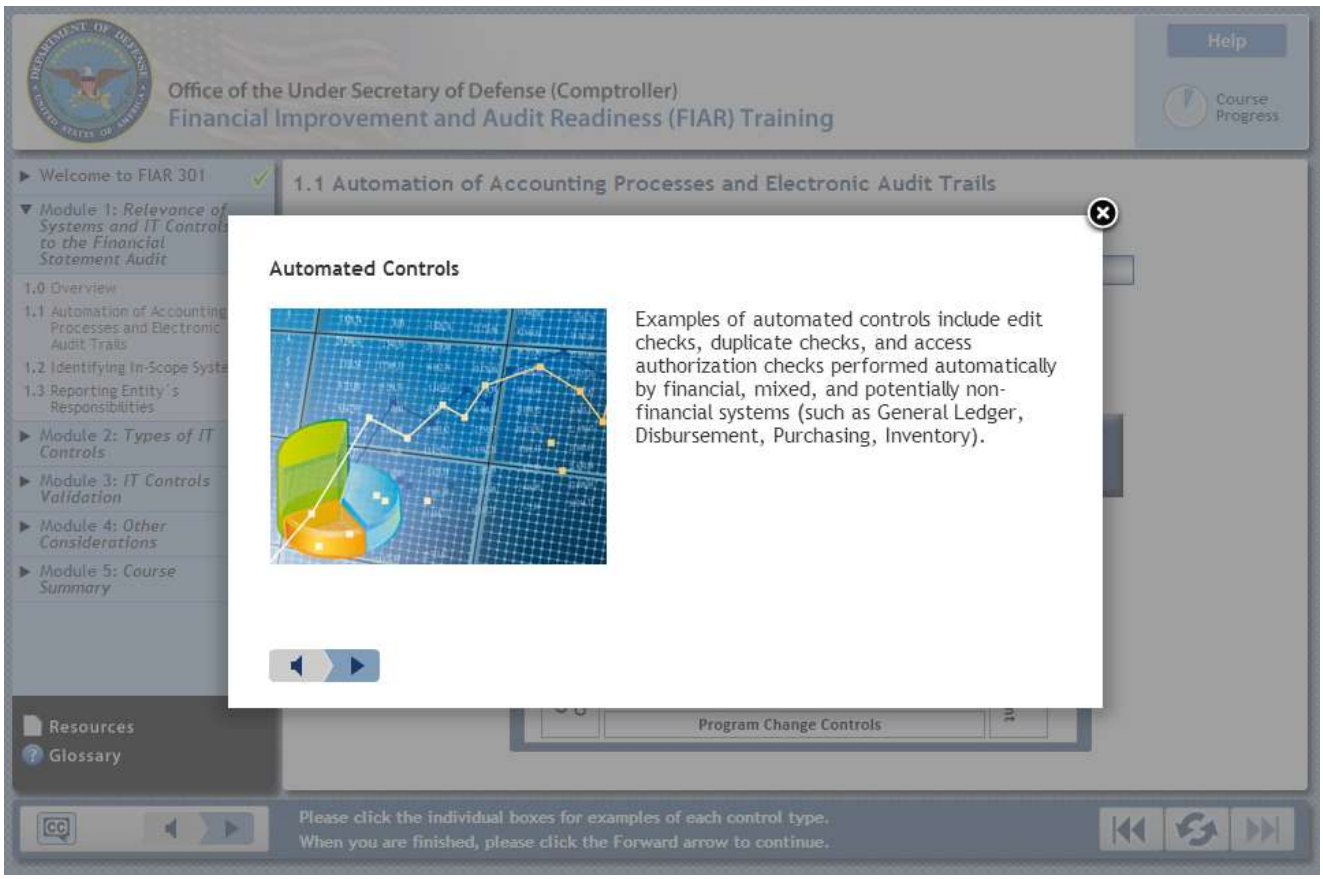
Within these processes, there are a number of Key Control Objectives - or KCOs - that need to be achieved to mitigate the risks of material misstatement and address the financial reporting assertions - Completeness, Existence, Valuation, Rights and Obligations and Presentation and Disclosure.

One or more control activities - or Key Controls - are performed to address the KCOs and corresponding financial reporting risks. These controls generally fall into one of the following three categories: Automated controls performed by the system, Manual controls that are performed using or are reliant upon system generated information, and strictly Manual controls not reliant on system generated information.

The DoD primarily uses automated controls and manual controls that rely on system-generated information.

When executing the FIAR Methodology, it is essential to recognize that if reliance is to be placed on automated controls and manual controls that rely on system generated reports or data, the reporting entity must obtain an understanding of, document, and test the IT general controls surrounding these systems. An ITGC environment must be in place before a reporting entity can rely on automated controls or manual controls that use system generated information.

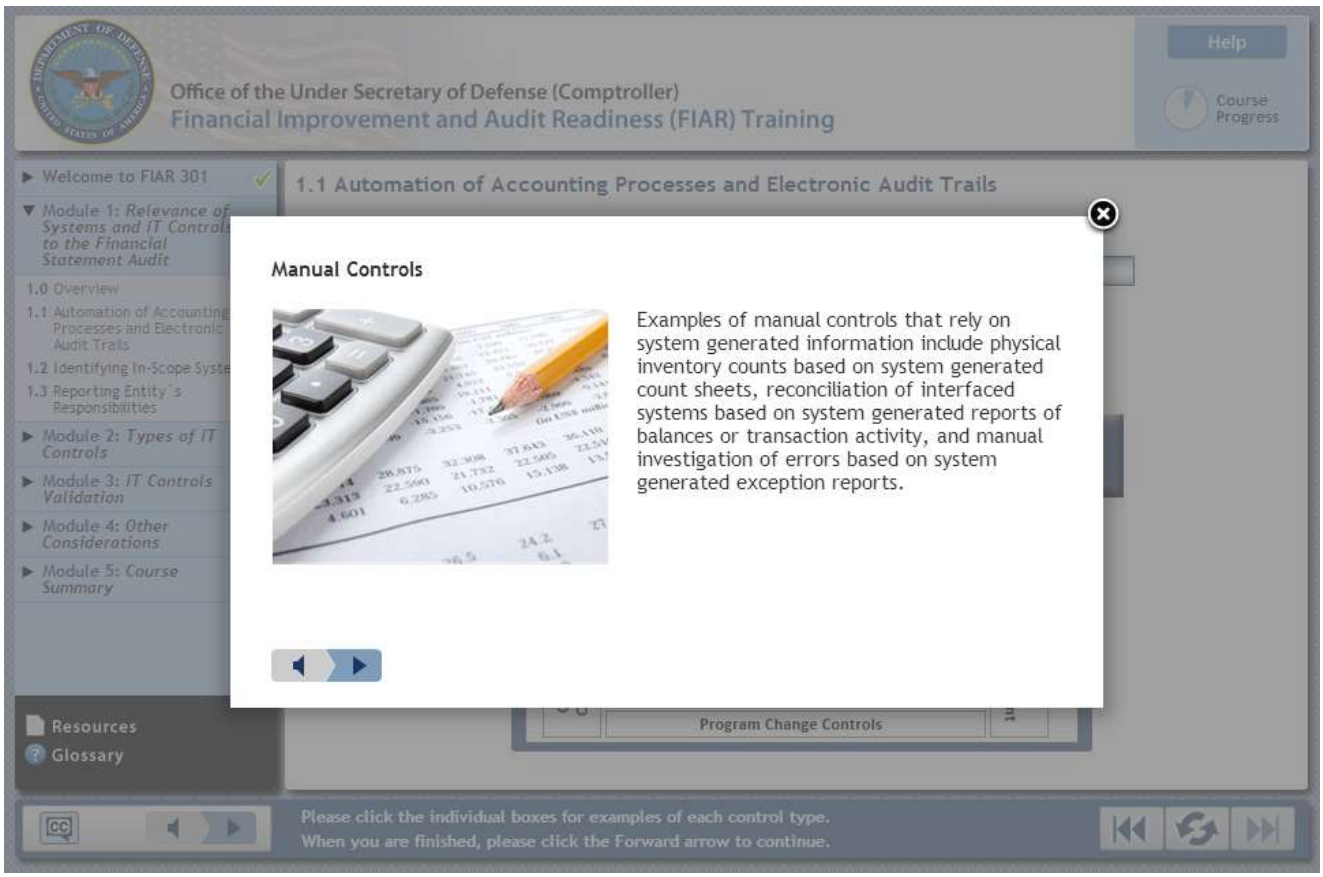
Please click the individual boxes for examples of each control type. When you are finished, please click the Forward arrow to continue.



Automated Controls

Examples of automated controls include edit checks, duplicate checks, and access authorization checks performed automatically by financial, mixed, and potentially non-financial systems - such as General Ledger, Disbursement, Purchasing, and Inventory.

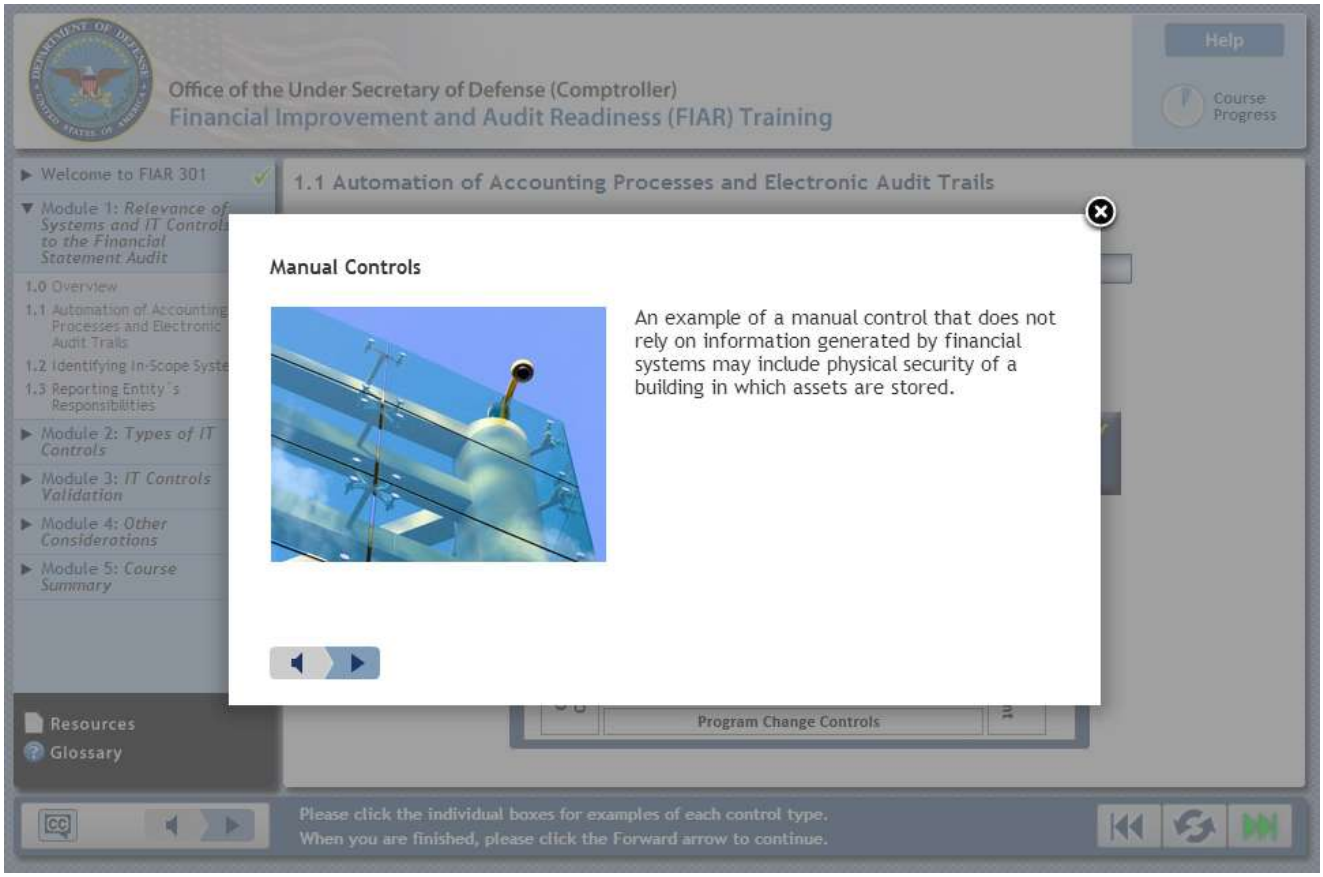
Please click the "X" in the upper-right corner to close this window and continue.



Manual Controls that rely on system generated information

Examples of manual controls that rely on system generated information include physical inventory counts based on system generated count sheets, reconciliation of interfaced systems based on system generated reports of balances or transaction activity, and manual investigation of errors based on system generated exception reports.

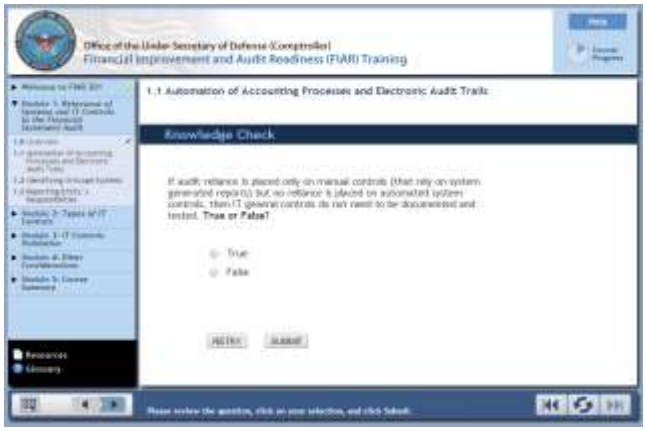
Please click the "X" in the upper-right corner to close this window and continue.

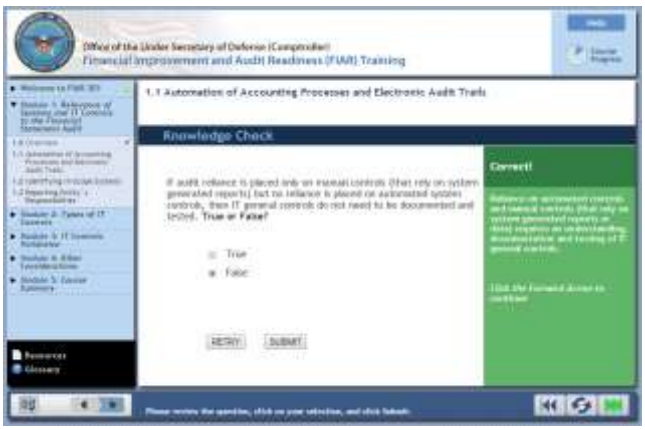


Manual Controls that do not rely on system generated information

An example of a manual control that does not rely on information generated by financial systems may include physical security of a building in which assets are stored.

Please click the "X" in the upper-right corner to close this window and continue.

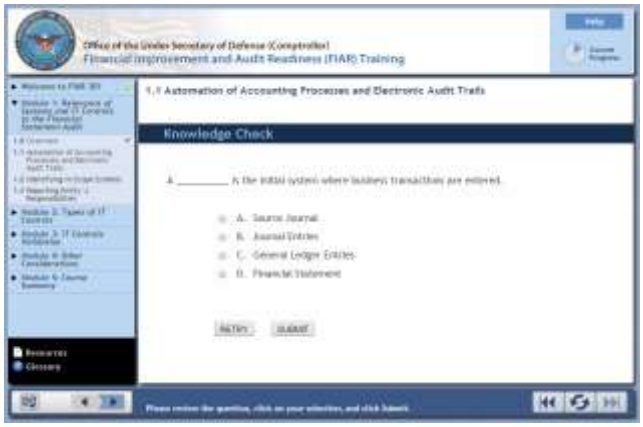


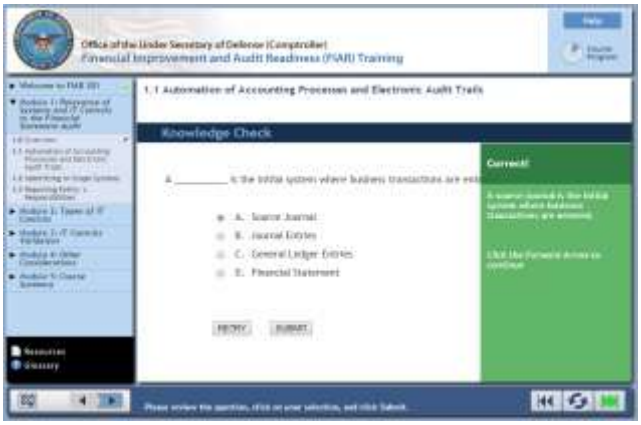


If audit reliance is placed only on manual controls (that rely on system generated reports) but no reliance is placed on automated system controls, then IT general controls do not need to be documented and tested. True or False?

Explanation

> ***False: Correct!*** *Reliance on automated controls and manual controls (that rely on system generated reports or data) requires an understanding, documentation and testing of IT general controls.*
>
> *True: Incorrect. Audit reliance should be placed on both manual and automated system controls.*



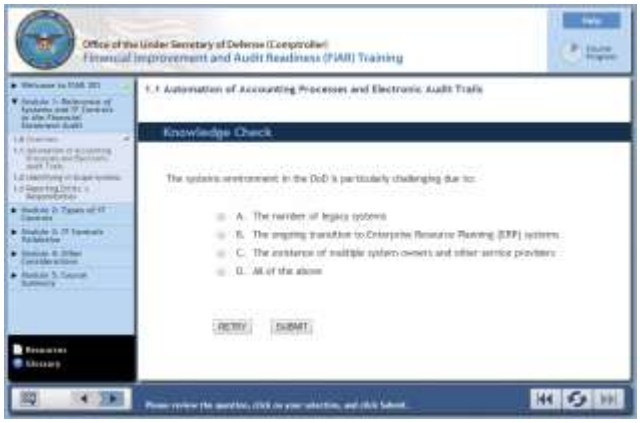


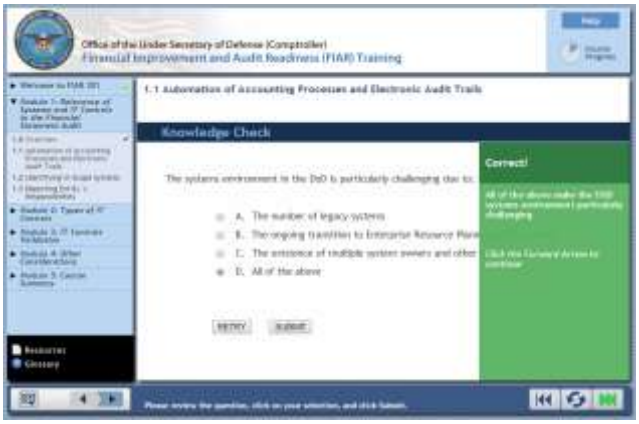
A _____ is the initial system where business transactions are entered.

a) Source Journal
b) Journal Entries
c) General Ledger Entries
d) Financial Statement

Explanation

a) Correct! A source journal is the initial system where business transactions are entered.
b) Incorrect. Journal entries are performed after the business transaction has been entered.
c) Incorrect. General ledger entries are performed after the business transaction has been entered.
d) Incorrect. Financial reporting (statements) is the last step for a business transaction.



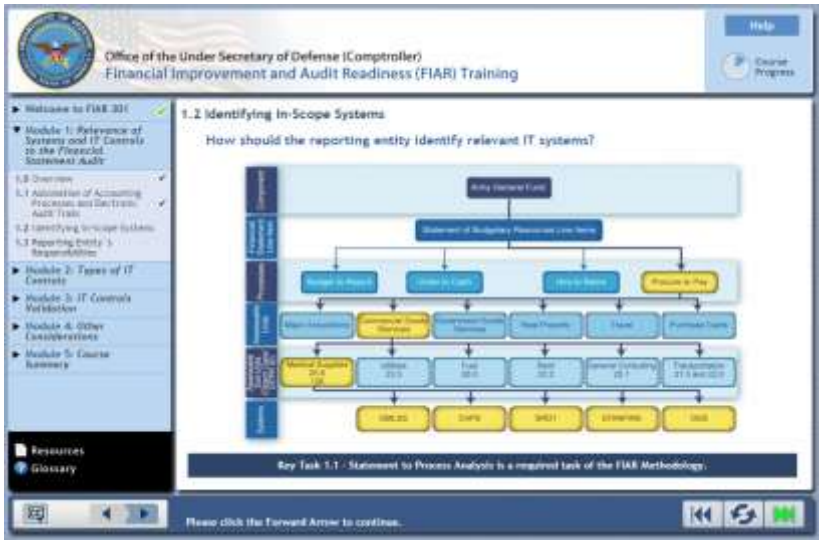


The systems environment in the DoD is particularly challenging due to:

a) The number of legacy systems
b) The ongoing transition to Enterprise Resource Planning (ERP) systems
c) The existence of multiple system owners and other service providers
d) All of the above

Explanation

a) Incorrect. Although the number of legacy systems is a challenge, it is not the only one.
b) Incorrect. Although the ongoing transition to ERPs is a challenge, it is not the only one.
c) Incorrect. Although the existence of multiple system owners and other service providers is a challenge, it is not the only one.
d) Correct! All of the above make the DOD systems environment particularly challenging.



1.2 Identifying In-Scope Systems

As you will recall from our operating supplies requisition example, we followed a transaction from initiation through general ledger posting and consolidation, and encountered a number of processes and systems.

The first key task of the Discovery Phase - 1.1 - is to perform a Statement to Process Analysis. Here, the Reporting Entity starts at the financial statement line item - in this case the Statement of Budgetary Resources' "Outlays" line item - and identifies the processes and systems that impact the line item and/or account balance. It is important to note that the Reporting Entity should include financial, mixed, and/or even non-financial applications if they support the transaction processing and/or execute key controls that impact the account or line item balance.

Financial applications are information systems that may perform all financial functions including general ledger management, funds management, payment management, receivable management, and cost management. Examples of financial systems include, but are not limited to: STANFINS, SOMARDS, STARS, GFEBS, NAVY ERP, GAFS-R, DEAMS, and DAI. Examples of payment management or disbursement systems include: ADS, SRD-1, DDS, and CDS.

Mixed applications are information systems that can support both financial and non-financial - or operational - functions. Examples include: DCPS and DJMS, which support the civilian and military payroll processes. These systems support both financial and operational aspects of payroll processing and reporting.

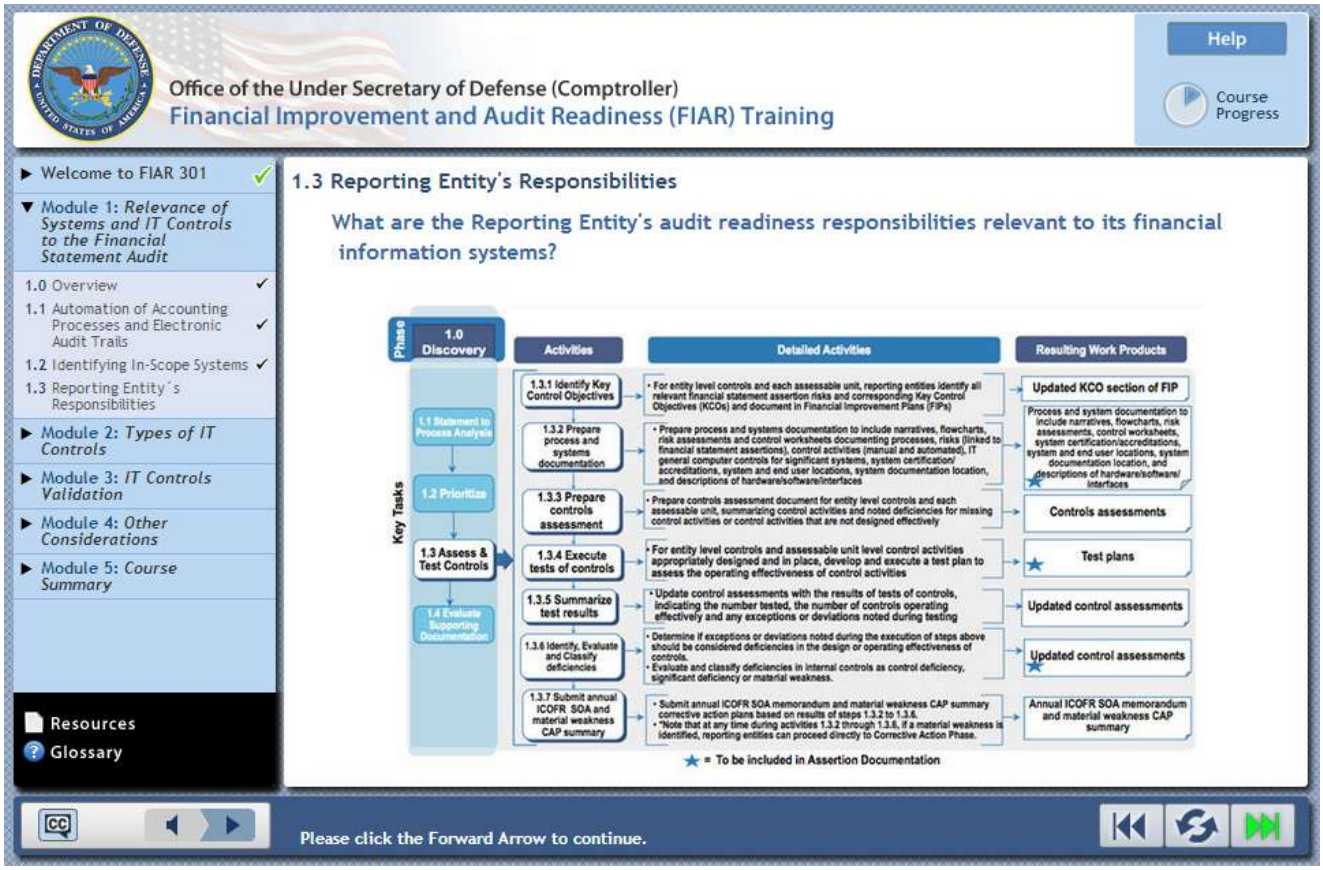
Non-financial applications are information systems that support non-financial functions and do not record financial events nor report financial information. However, non-financial systems may be relevant for financial reporting and audit readiness as they may house financially relevant data that could be later processed by a financial or mixed system to report financial information in the financial systems. For example, DCPDS, the personnel system, does not perform financial functions, but is relevant to the internal controls for the civilian pay business process (assessable unit) because it is the source system for employee master data that contains financially relevant information, such as pay rates, and drives the payroll calculation performed by DCPS.

In this example, we focus on the "Procure to Pay" process which supports the outlays line item in the SBR. Other business processes that impact the SBR are:

Hire-to-Retire - including payroll; Order-to-Cash - also referred to as Order-to-Fulfill; and Budget-to-Report

Once the Reporting Entity has identified the universe of systems that contribute to an account or line item balance, the Reporting entity needs to determine the relevance of the system for audit readiness purposes and prioritize the order for performing audit readiness and internal control over financial reporting activities over each system - Key Task 1.2 in the Discovery Phase.

Please click the Forward arrow to continue.



1.3 Reporting Entity's Responsibilities

Once Reporting Entities have identified and prioritized the relevant IT application and general controls, they will then move on to Key Task 1.3 to assess and test the controls to address internal control over financial reporting and audit readiness considerations.

The activities within "Assess and Test Controls" are:

Task 1.3 - Assess and Test Controls -- this is covered extensively is FIAR 102

Activity 1.3.1 - Identify Key Control Objectives - as well as financial statement risks of material misstatement

Activity 1.3.2 - Prepare Process and Systems Documentation

Activity 1.3.3 - Prepare Controls Assessment

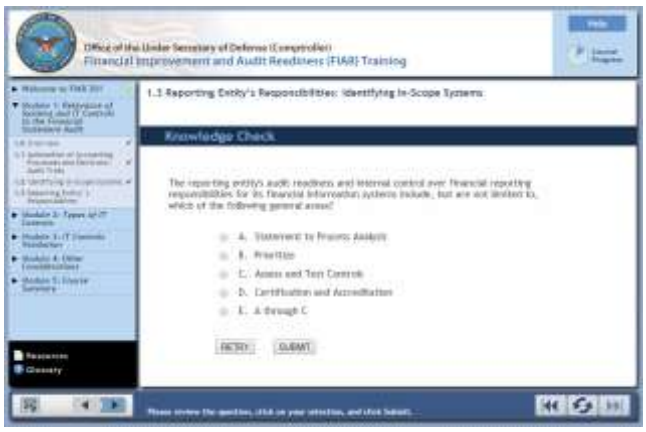
Activity 1.3.4 - Execute Tests of Controls

Activity 1.3.5 - Summarize Test Results

Activity 1.3.6 - Identify, Evaluate, and Classify Deficiencies

Activity 1.3.7 - Submit Annual ICOFR SOA and Material Weakness Corrective Action Plan (or CAP) Summary

Please click the Forward arrow to continue.

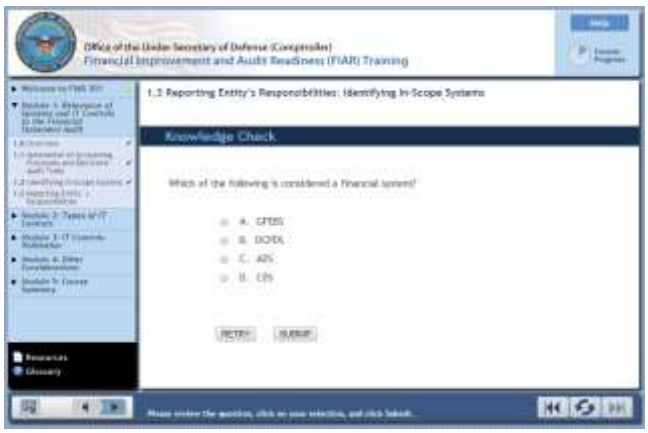


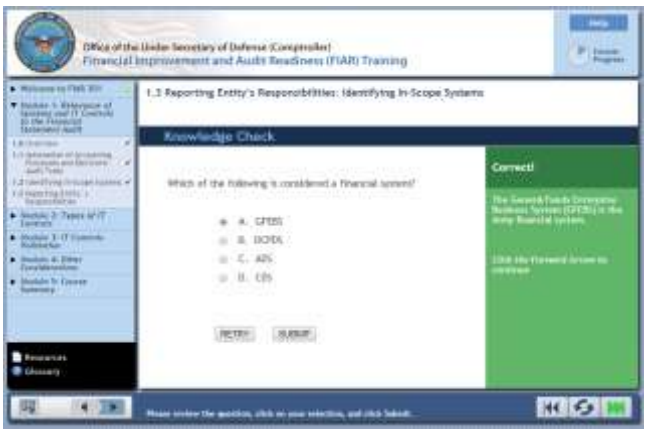
The reporting entity's audit readiness and internal control over financial reporting responsibilities for its financial information systems include, but are not limited to, which of the following general areas?

a) Statement to Process Analysis
b) Prioritize
c) Assess and Test Controls
d) Certification and Accreditation
e) A through C

Explanation

a) Incorrect. Statement to Process Analysis is only one area that is the reporting entity's audit readiness and internal control over financial reporting responsibilities.
b) Incorrect. Prioritize is only one area that is the reporting entity's audit readiness and internal control over financial reporting responsibilities.
c) Incorrect. Assess and Test Controls is only one area that is the reporting entity's audit readiness and internal control over financial reporting responsibilities.
d) Incorrect. While system certification and accreditation is an important DoD compliance requirement, it is not a specific requirement for audit readiness or internal controls.
e) Correct! Statement to Process Analysis, Prioritize and Assess and Test Controls are all the reporting entity's audit readiness and internal control over financial reporting responsibilities.





Which of the following is considered a financial system?

a) GFEBS
b) DCPDS
c) ADS
d) CDS

Explanation

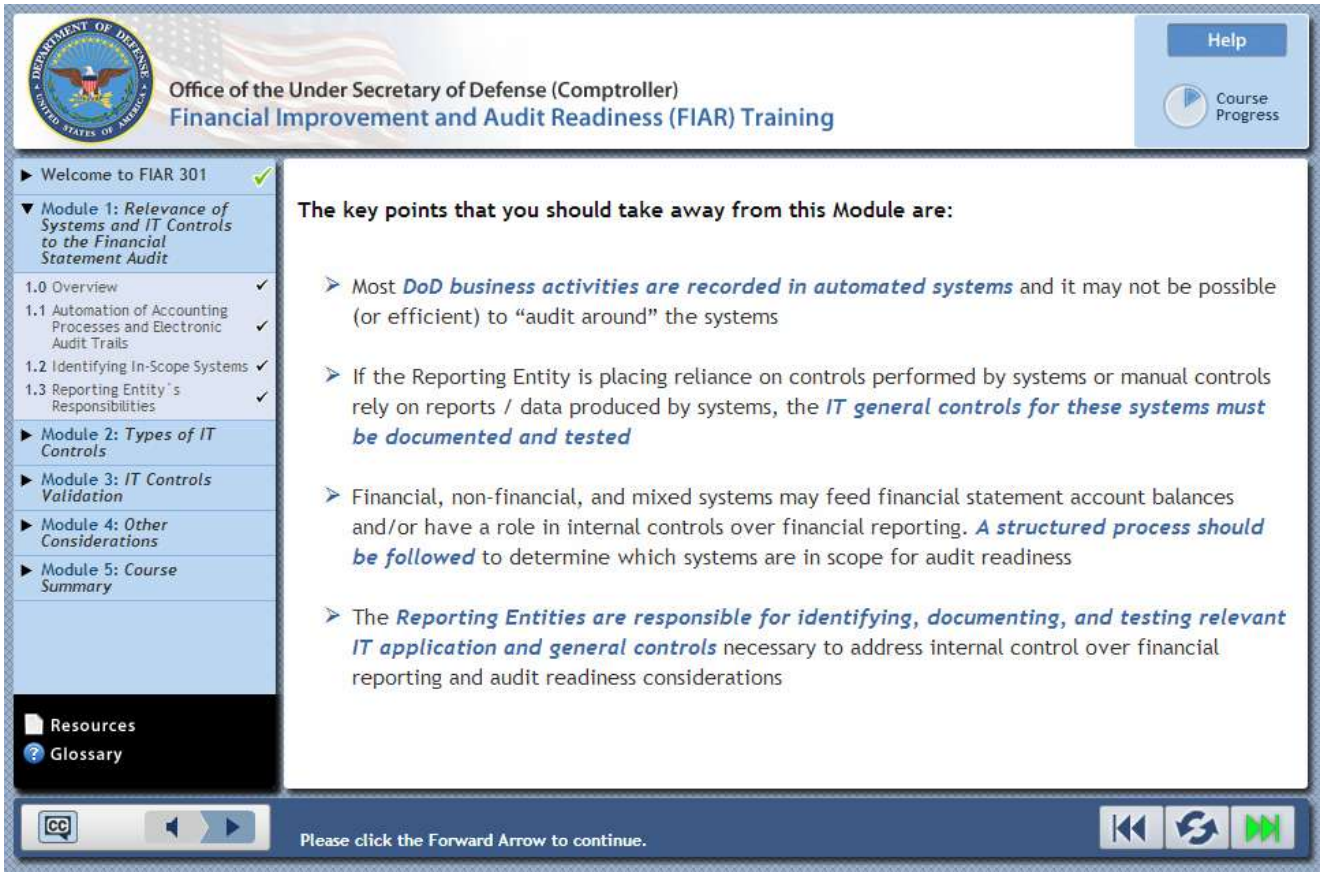
a) Correct! The General Funds Enterprise Business System (GFEBS) is the Army financial system.
b) Incorrect. The Defense Civilian Personnel Data System (DCPDS) is a non-financial system.
c) Incorrect. The Automated Disbursing System (ADS) is considered a mixed (both financial and non-financial) system.
d) Incorrect. The Contractor Debt System (CDS) is considered a mixed (both financial and non-financial) system.

The reporting entity's audit readiness and internal control over financial reporting responsibilities for its financial information systems include, but are not limited to, which of the following general areas?

a) Hire-to-Retire
b) Order-to-Cash
c) Procure-to-Pay
d) Budget-to-Report
e) All of the above

Explanation

a) Incorrect. There is more than one business process that impacts the SBR and therefore, this answer is incorrect.
b) Incorrect. There is more than one business process that impacts the SBR and therefore, this answer is incorrect.
c) Incorrect. There is more than one business process that impacts the SBR and therefore, this answer is incorrect.
d) Incorrect. There is more than one business process that impacts the SBR and therefore, this answer is incorrect.
e) Correct! A, B, C, and D are all business processes that impact the SBR.



Module 1 Summary

After completing this module, you should now understand and be able to apply the following:

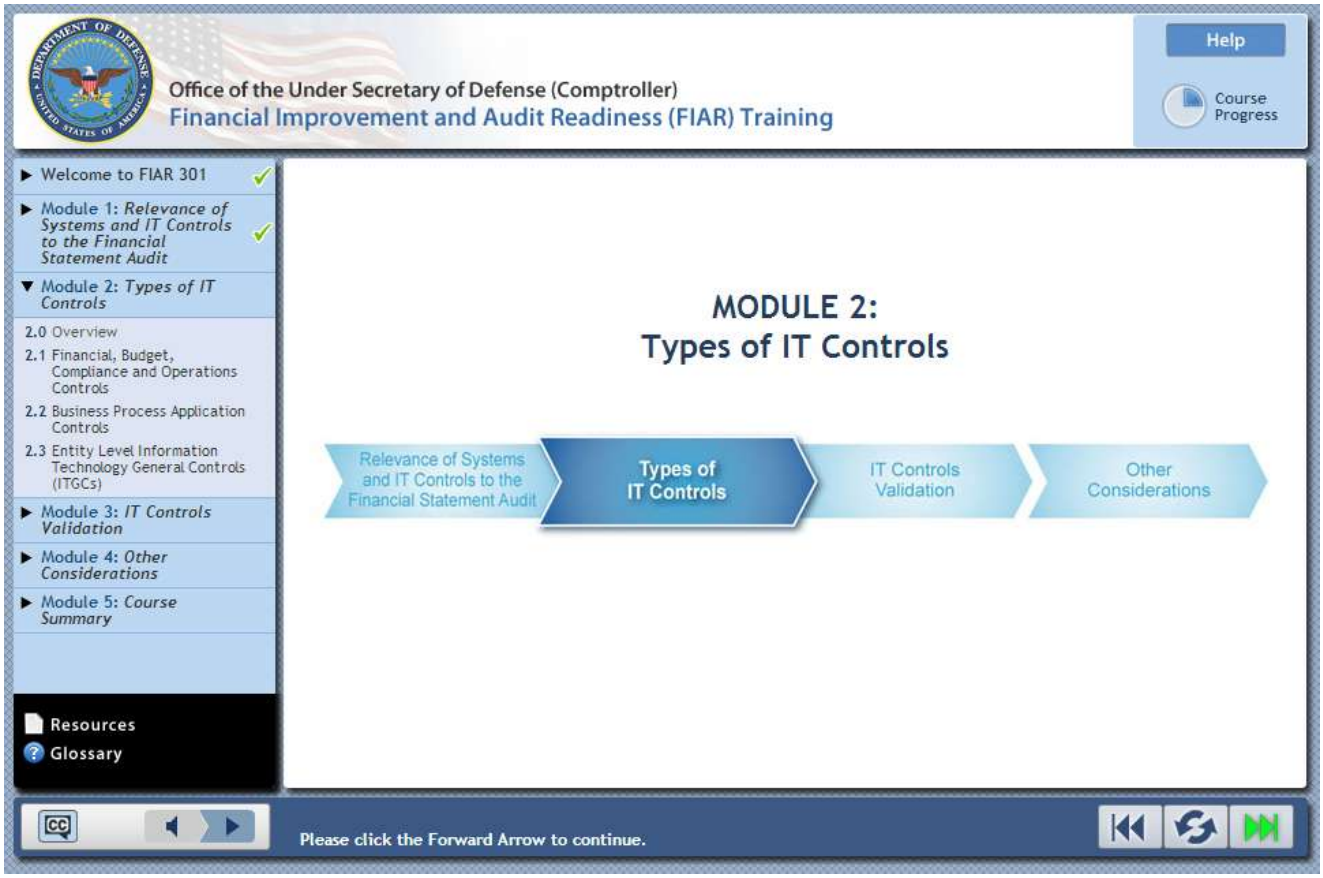
Today, most DoD business transactions are recorded in computerized information systems and the DoD has a very complex and evolving systems environment. The flow of information from point of transaction initiation in source journals through posting in the general ledger and consolidation systems generally occurs electronically and supporting documentation may only exist in an electronic format. Given this dependence on computerized systems, it may not be possible to "audit around" these systems as physical source documentation may not exist. Even in those instances where it may be possible to "audit around" the Department's information systems, it will likely be inefficient to do so given the high volume of transactions and correspondingly large number of sample sizes required to audit around the system.

It is essential to recognize that reliance on automated controls and manual controls that rely on system generated reports or data requires an understanding, documentation, and testing of IT general controls.

Financial, non-financial, and mixed systems may impact financial statement account balances and/or have a role in internal controls over financial reporting. A structured process should be followed to determine which systems are in scope for audit readiness. This process should include the Statement to Process Analysis and Prioritize Key Tasks 1.1 and 1.2.

The Reporting Entities are responsible for identifying, documenting, and testing relevant IT application and general controls necessary to address internal control over financial reporting and audit readiness considerations.

Please click the Forward arrow to continue.



Module 2 Intro: Types of IT Controls

Now we will begin Module 2. This module introduces the types of IT controls and their relevance to audit readiness.

Please click the Forward arrow to continue.

2.1 Financial, Budget, Compliance and Operations Controls

Let's take a look at the four types of general control categories:

Operational or Operations Controls provide reasonable assurance that the Reporting Entity achieves the performance desired by management for planning, productivity, quality, economy, efficiency, or effectiveness of the entity's operation.

In our purchase/requisition example earlier, an operational/non-financial control might be actions taken to make sure the truck ordered and delivered has the necessary payload capacity to meet operational requirements.

Compliance Controls provide reasonable assurance that the Reporting Entity complies with significant provisions of applicable laws and regulations.

In our purchase/requisition example, a compliance control might be the requirement for a Disbursing Officer to review and approve the disbursement package - ensuring proper supporting documentation for receipt and acceptance exists - before payment is made to the truck vendor.

Budget Controls, also known as Funds Control, execute transactions in accordance with budget authority.

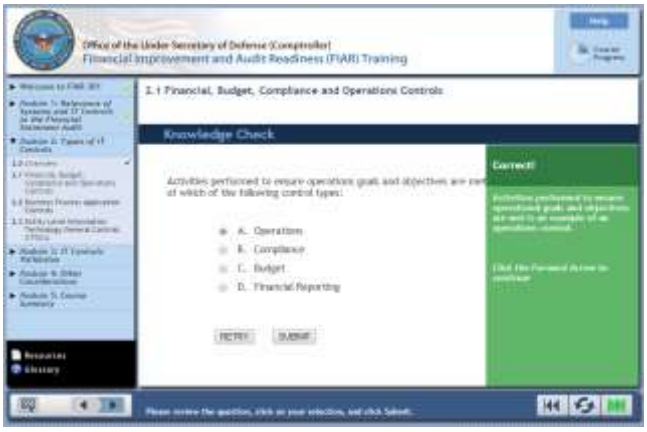
In our purchase/requisition example, a budget control would be a Budget Officer ensuring that sufficient funds are available before placing an order for additional trucks (per the Grassley Act).

Financial Reporting Controls are identified by reporting entities when designing their systems. The reporting entities identify control objectives for each type of control that, if achieved, would provide the entity with reasonable assurance that individual and aggregate misstatements (whether caused by error or fraud), losses, or noncompliance material to the financial statements would be prevented or detected and corrected. These include safeguarding controls to protect assets against loss from unauthorized acquisition, use, or disposition, and segregation of duties controls to prevent one person from controlling multiple aspects of a transaction allowing that person to both cause and conceal misstatements (whether errors or fraud).

In our purchase/requisition example, an example of a financial reporting control would be a procurement officer reviewing an approved purchase order or contract for accuracy prior to recording an obligation in the financial system. Financial reporting controls include those activities that are performed to ensure financial reporting objectives are met and financial statements are prepared in accordance with GAAP.

Because the emphasis of this course is on audit readiness and the associated internal controls over financial reporting, it is important to recognize that certain operational, compliance, and/or budgetary controls could also be leveraged to address relevant financial reporting and audit readiness control objectives. For example, custody over and tracking the location of physical assets is an operational control that is also important for internal controls over financial reporting (specifically, the existence assertion).

Please click the Forward arrow to continue.

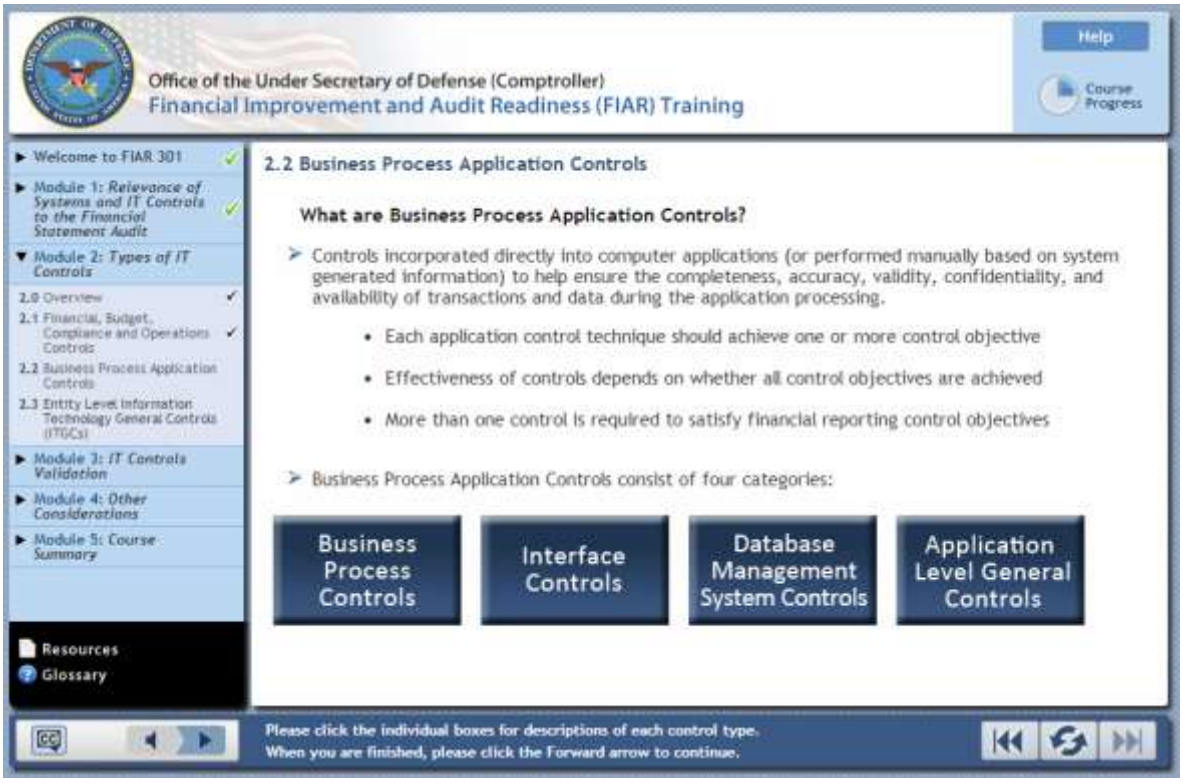


Activities performed to ensure operations goals and objectives are met is an example of which of the following control types:

a) Operations
b) Compliance
c) Budget
d) Financial Reporting

Explanation

a) Correct! Activities performed to ensure operational goals and objectives are met is an example of an operations control.
b) Incorrect. Activities performed to ensure the DoD is in compliance with applicable laws, regulations, and directives is an example of a compliance control.
c) Incorrect. Activities performed to ensure proper budget formulation and execution is an example of a budget control.
d) Incorrect. Activities performed to ensure ICOFR objectives are met and financial statements are prepared in accordance with generally accepted accounting principles is an example of a financial reporting control.



2.2 Business Process Application Controls

The overall objective of business process application controls is to provide reasonable assurance about the completeness, accuracy, validity, confidentiality, and availability of transactions and data during application processing.

The reporting entity should design each specific business process application control technique to achieve one or more control objectives. It is important to remember that the effectiveness of business process application controls depends on whether all of these overall objectives are achieved.

As noted earlier in the purchase/requisition example, an example of a business process application control is user access restrictions in applications that only allow authorized personnel to enter transactions. This control would address the validity objective. If the relevant software applications also include automated edit checks to ensure that all required screen fields are completed and checks the data entered against allowed values, the completeness and accuracy objectives would be addressed as well.

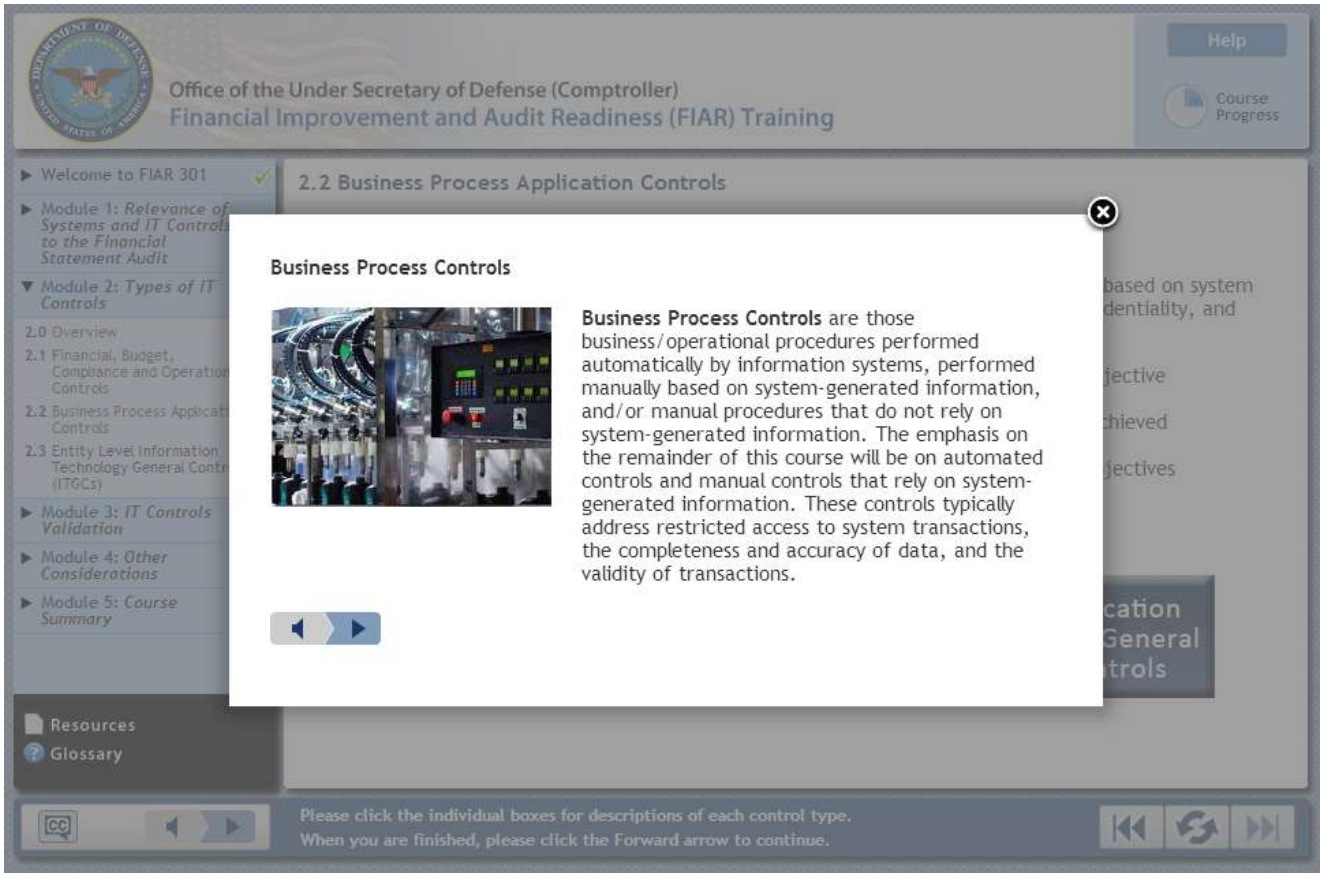
Typically, more than one control is required to satisfy financial reporting control objectives for the entire business process.

Business Process Application Controls consist of the following four categories:

- Business Process Controls;
- Interface controls;
- Database Management System Controls; and,
- Application Level General Controls

Examples of each of the categories of controls are provided on the following pages using our truck requisition scenario.

Please click the individual boxes for descriptions of each control type. When you are finished, please click the Forward arrow to continue.



Business Process Controls

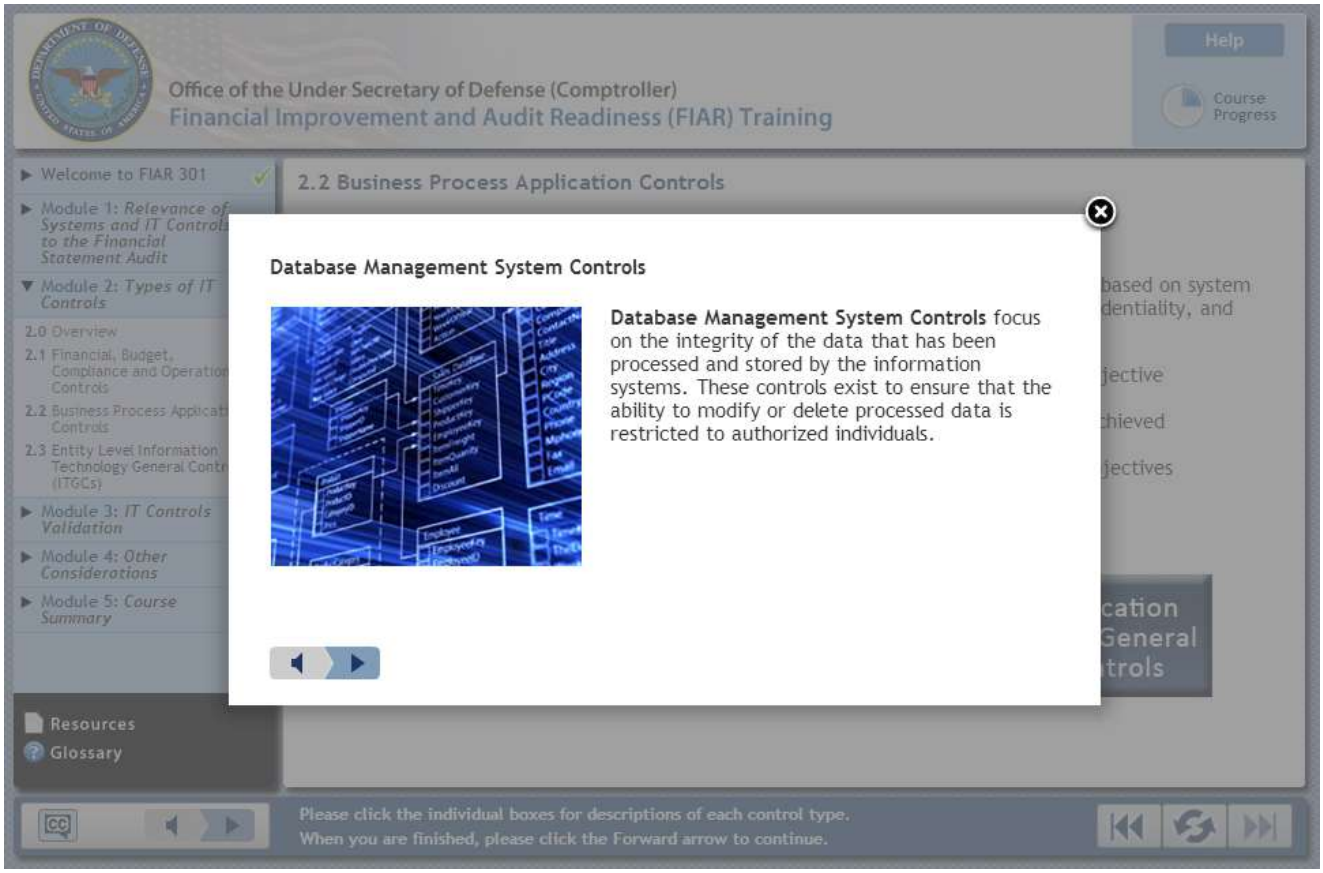
Business Process Controls are those business an operational procedures performed automatically by information systems, performed manually based on system-generated information, and/or manual procedures that do not rely on system-generated information. The emphasis on the remainder of this course will be on automated controls and manual controls that rely on system-generated information. These controls typically address restricted access to system transactions, the completeness and accuracy of data, and the validity of transactions.

Please click the “X” in the upper-right corner to close this window and continue.

Interface Controls

Interface controls focus on the exchange of data between information systems and are primarily concerned with the completeness and accuracy of the data exchanged.

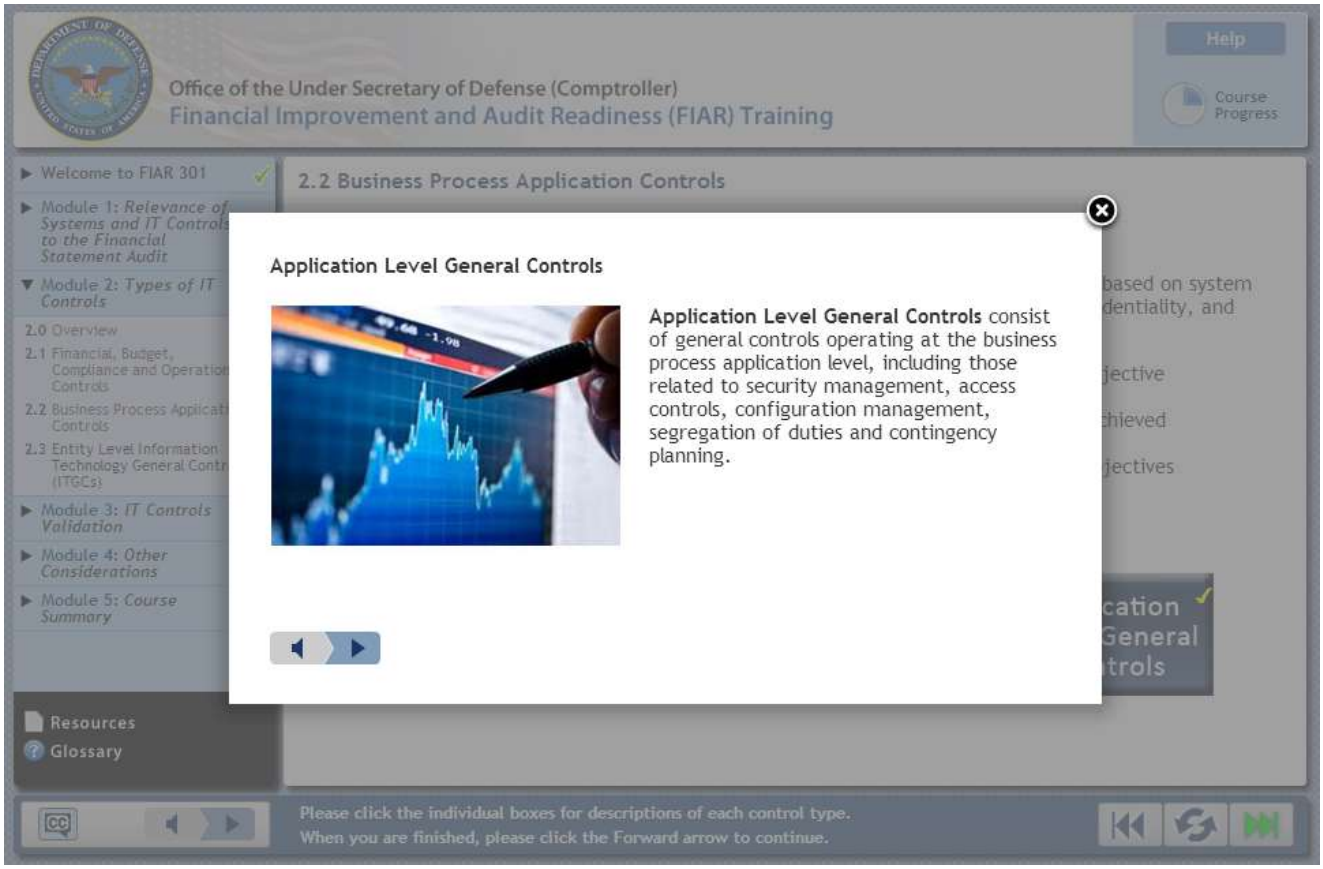
Please click the “X” in the upper-right corner to close this window and continue.



Database Management System Controls

Database Management System Controls focus on the integrity of the data that has been processed and stored by the information systems. These controls exist to ensure that the ability to modify or delete processed data is restricted to authorized individuals.

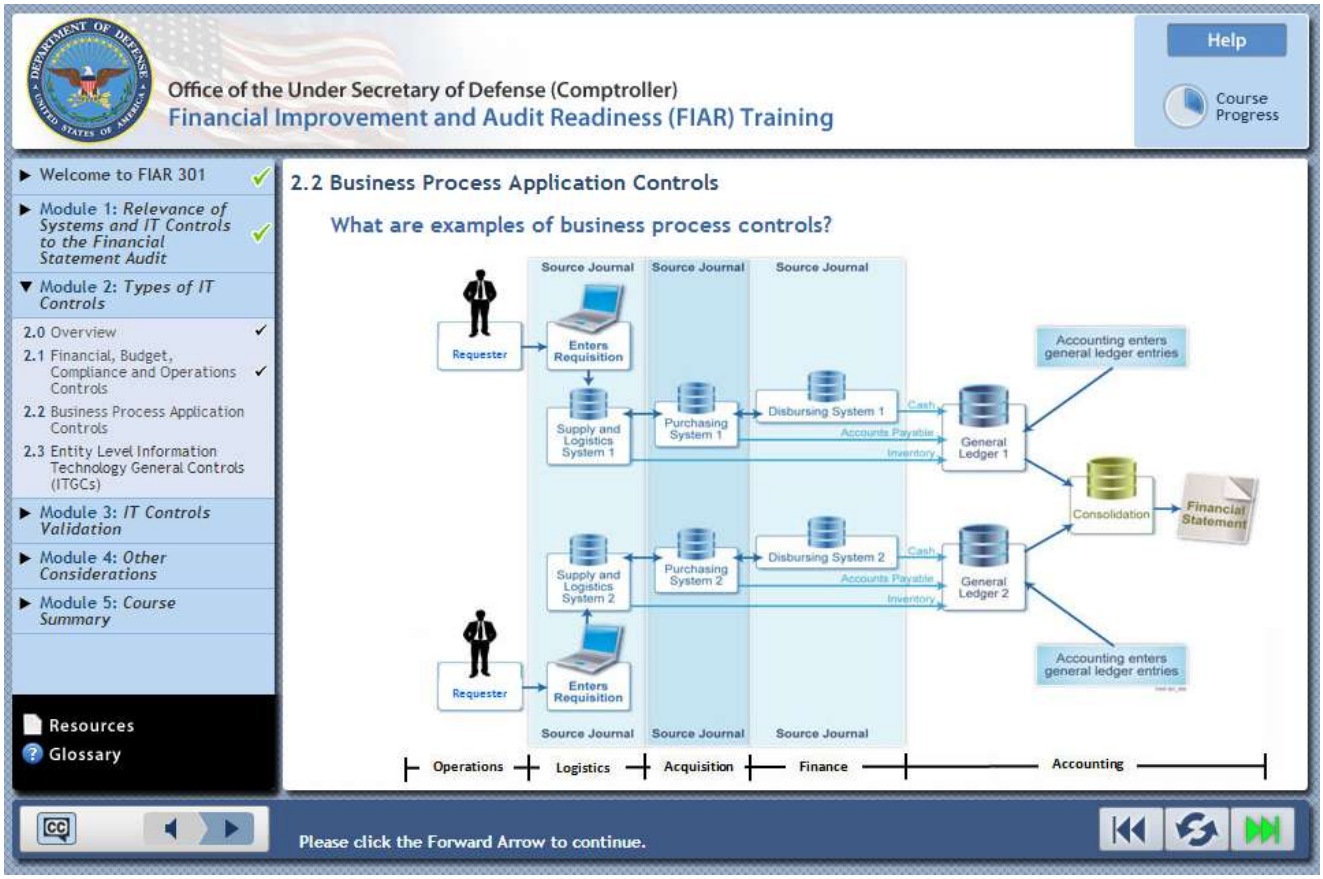
Please click the “X” in the upper-right corner to close this window and continue.



Application Level General Controls

Application Level General Controls consist of general controls operating at the business process application level, including those related to security management, access controls, configuration management, segregation of duties and contingency planning.

Please click the “X” in the upper-right corner to close this window and continue.



What are examples of business process controls?

Let's return to our illustration again, this time to review examples of business process controls which include:

Access Controls - Software applications are CAC enabled and/or have user-id and passwords that prevent unauthorized access to systems.

Segregation of Duties Controls - Procedures ensure individuals are not granted incompatible or conflicting access privileges – such as transactions, roles, or profiles - in an application or across multiple applications. For example, it would be inappropriate for an individual to have unrestricted access to the requisitioning, purchasing, S&L, Disbursing and GL system allowing him or her to execute all of the following business activities:

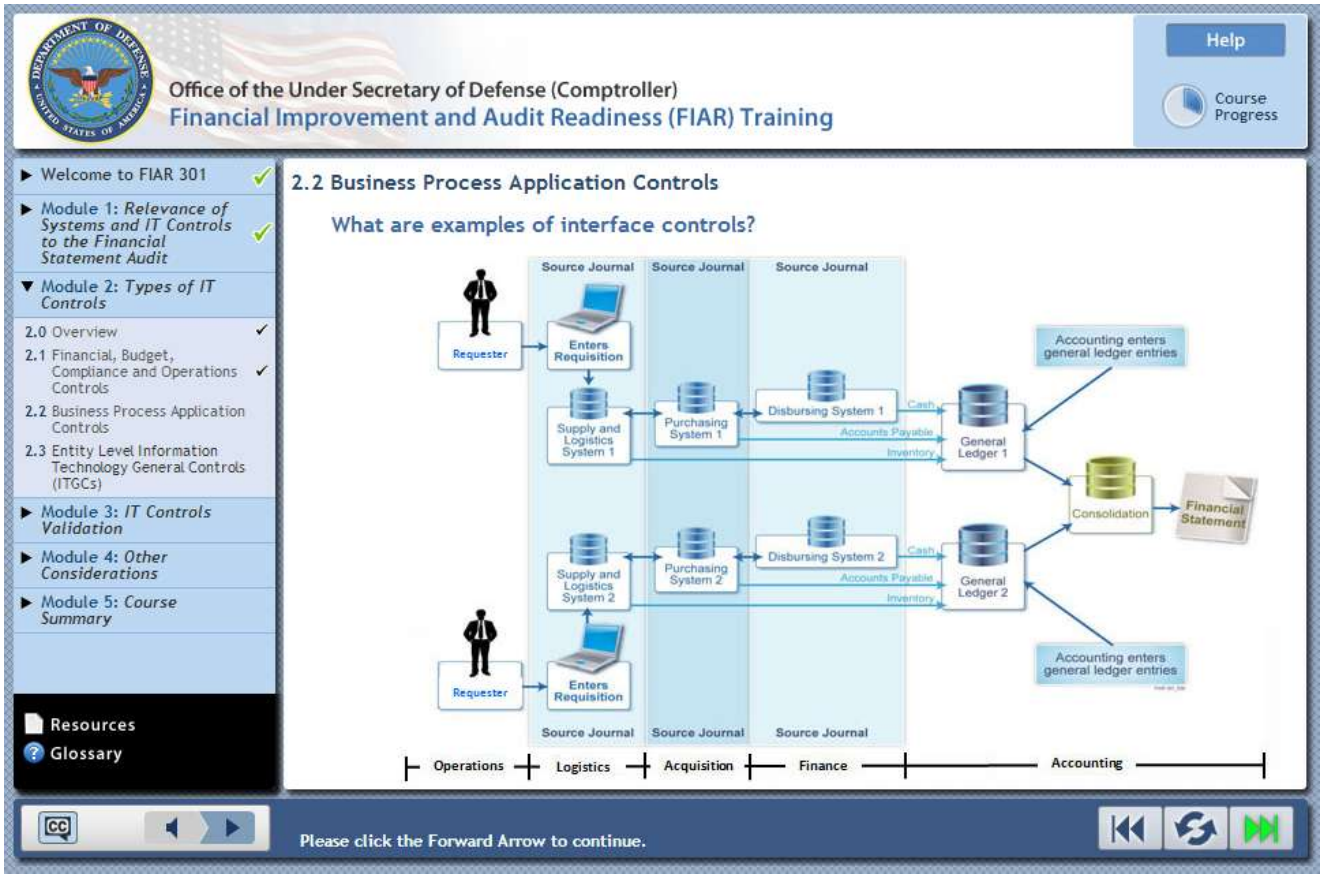
- Create a vendor; Create a purchase order; Create or approve goods or services receipt; Enter and approve an invoice; or Approve or process a disbursement.

Granting all of the above access privileges to a single individual gives that person the ability to create fictitious, unauthorized, and potentially fraudulent transactions because he has the system privileges necessary to circumvent internal controls.

In addition, periodic physical inventory counts should be performed by an individual not responsible for the day-to-day physical custody of assets, to confirm the existence and location of assets as recorded in inventory systems and the general ledger. This is another example of a segregation of duties control.

Edit Checks - The requisitioning system may be configured to require the user to input all required data fields before saving a requisition. The edit check is an example of a completeness control.

Please click the Forward arrow to continue.



What are examples of interface controls?

An example of interface controls is when there is an automated control - or manual control based on system generated information - that checks to see if the total number of records have been transferred from the purchasing system to the entitlement/disbursing system.

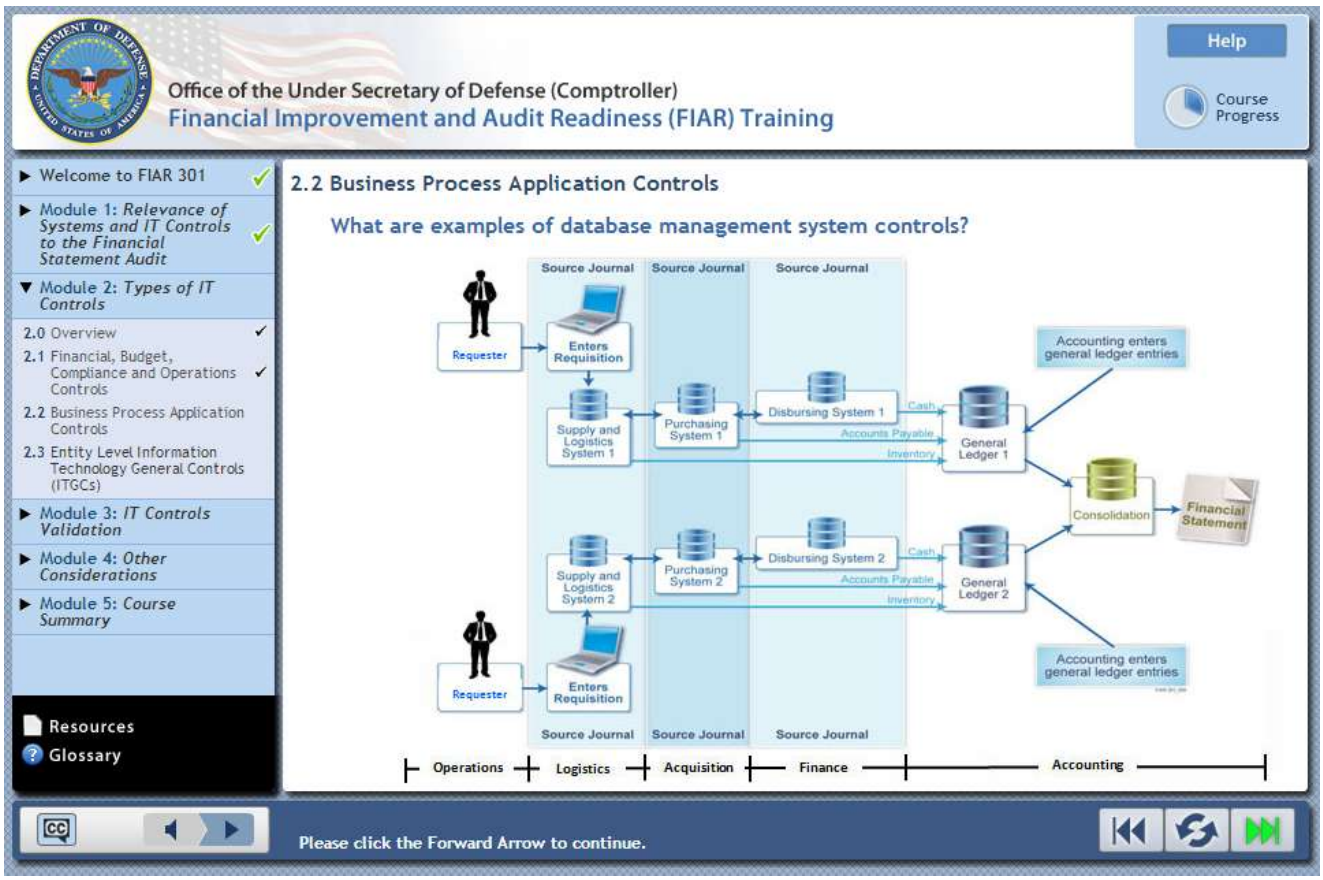
Periodic reconciliations of the supply and logistics system, purchasing system, and disbursing system to the general ledger balances should be performed to ensure that all financial data is accurately and completely flowing through the numerous systems. Performing this reconciliation will address the completeness and accuracy assertion.

It is important to note that in the simplified example that we have been using, there are a total of 18 system-to-system interfaces.

As legacy systems are replaced by integrated Enterprise Resource Planning - or ERP - systems, we would expect to see a reduction in the number of interfaces.

While there may be an automated interface control, the reporting entity must identify and test the relevant manual control as well. For example, an analyst identifies and resolves the errors related to the interface and then a supervisor verifies the reasonableness of the analyst's work and signs off.

Please click the Forward arrow to continue.



What are examples of database management system controls?

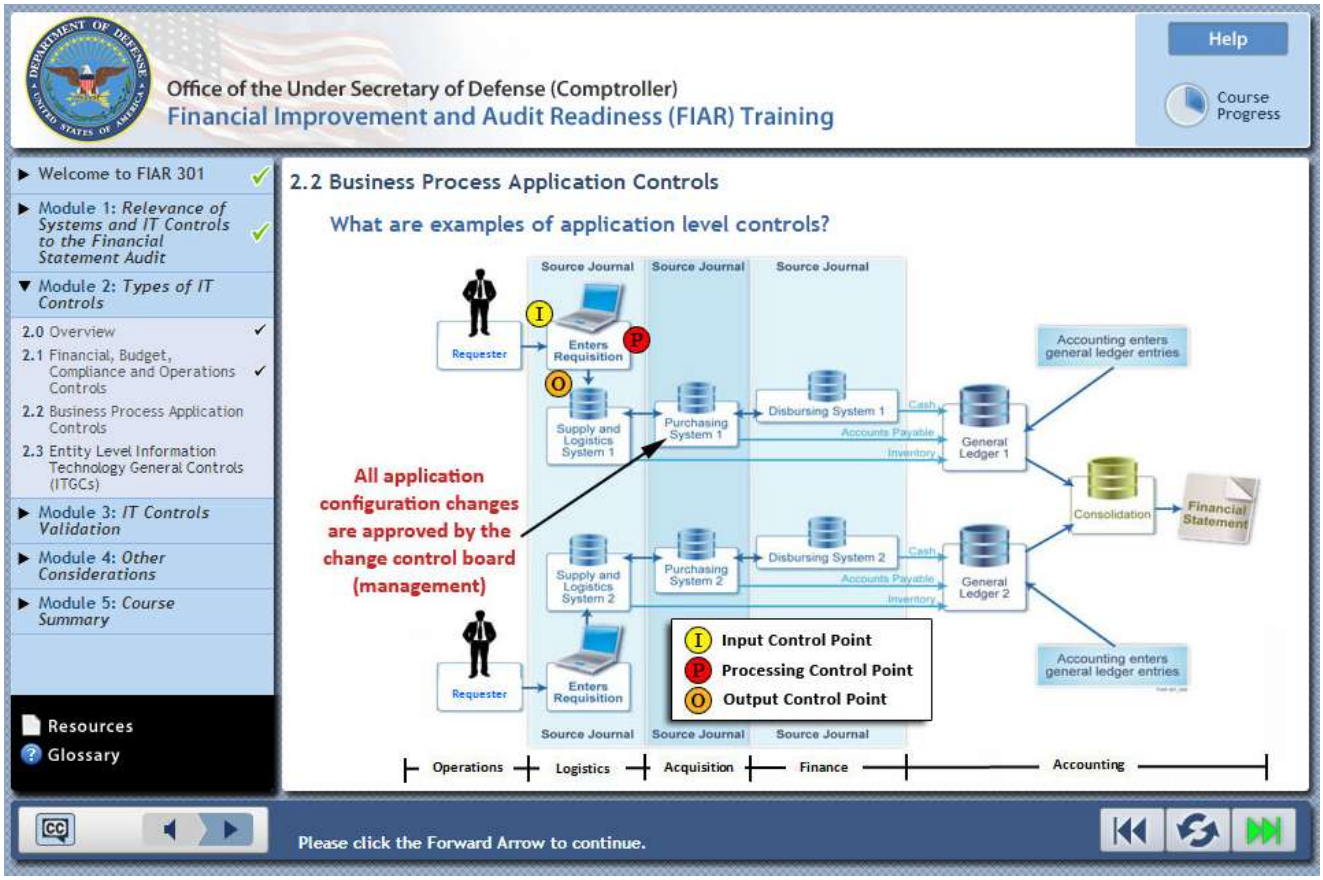
An example of a Database Management System Control is when security settings and assigned access privileges prevent software developers from directly changing data that is stored by the general ledger application in an underlying database management or electronic file storage system.

This is important because developers and database administrators should not be authorized to process accounting transactions. If these individuals have direct access to modify the underlying financial data, they could circumvent this access restriction to enter unauthorized transactions. Furthermore, the information entered would not pass through the "official" system of record and not be subject to normal system validity checks.

It is important to note that in the simplified example we have been following, **EACH** legacy system would likely have its own separate database or file storage system.

In an ERP environment, the functions performed by one or more separate legacy systems would be performed by modules of the ERP system. The key difference is ERP system modules typically share a single common integrated database which means the data is only entered once.

Please click the Forward arrow to continue.



What are examples of application level controls?

Input Controls are designed to reasonably ensure that: all data input is done so in a controlled manner; data input into an application is complete, accurate and valid; any incorrect information is identified, rejected and corrected; and the confidentiality of the data is protected. Examples of input controls include automated edit checks to ensure that all required data fields have been populated, the dollar value of transactions entered may be limited or restricted by a user's job role or level, and users who enter transactions are not also able to approve and certify them.

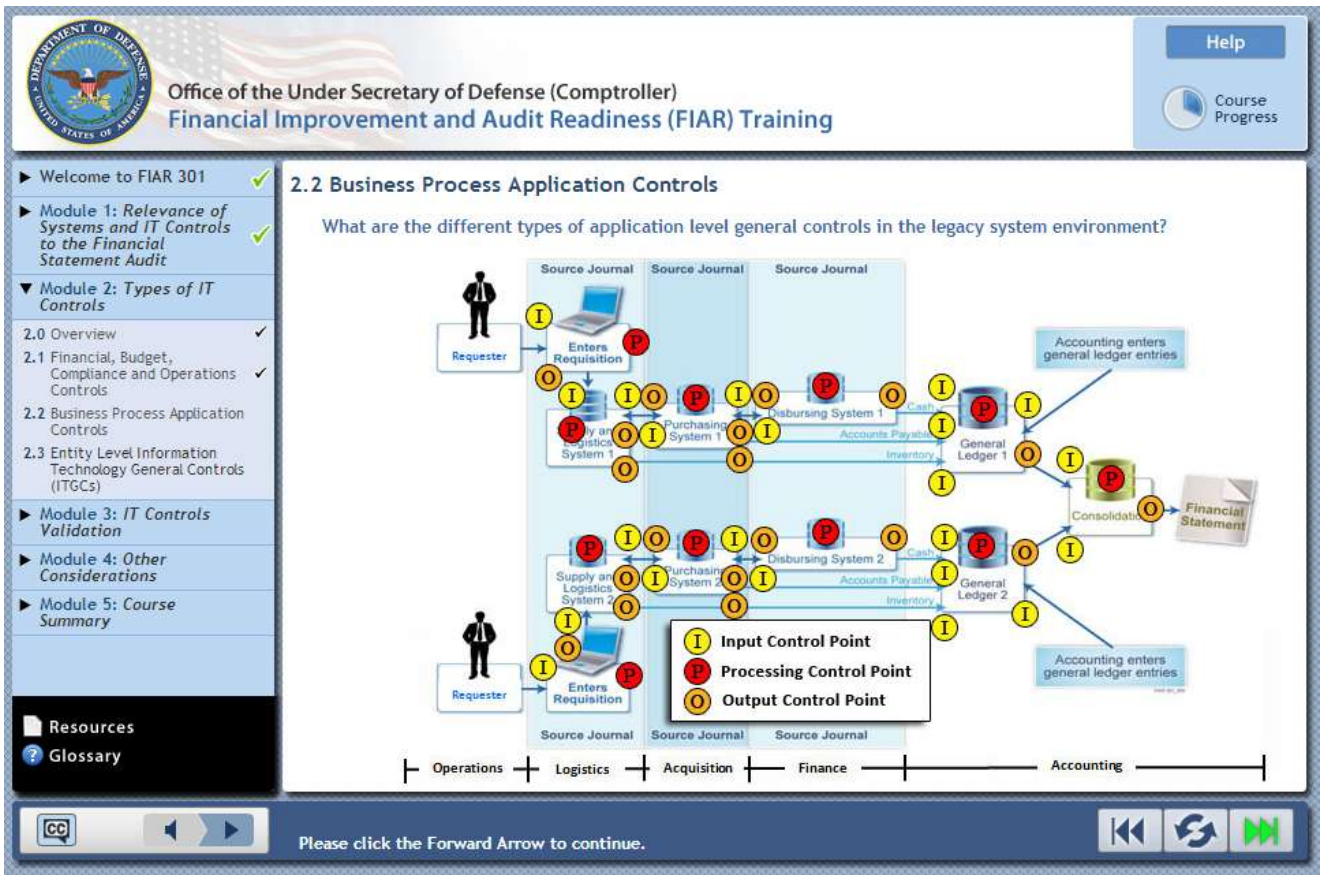
Processing Controls address the completeness, accuracy, validity, and confidentiality of data as the data gets processed within the applications. Examples of processing controls may include system performed checks to ensure all records input were actually processed (such as comparing number of records input to number of records output), maintaining a transaction processing log which provides an audit trail, and the ability to compare processed financial data and transactions to the source documents. The processing logs could also be used to identify those transactions that did not process completely or accurately within the application.

Output Controls are used to reasonably assure that transaction data is complete, accurate, valid and confidential. In addition, output controls are aimed at the correct and timely distribution of any output produced. Examples include restricting logical or physical access to system output files to ensure data is not modified before it is uploaded into a downstream application for further processing.

An example of an application level general control is changes to the application purchasing system configuration must be approved by the organizations' designated Change Control Board before a change is made.

Business management needs to approve all changes to identify potential cross system impact; to ensure continued compliance with laws and regulations; to prevent unscheduled downtime; and to be able to rely on the application to function the same way from one day to the next.

Please click the Forward arrow to continue.



What are the different types of application level general controls in the legacy system environment?

As data flows through the individual legacy systems - whether entered manually or via automated interface - multiple input, processing, and output activities are introduced. Each of these input, processing, and output points need to be controlled to ensure the completeness, accuracy, and validity of the transaction data. These are application controls. In our illustration, we've identified three types of controls – Input Control Points, marked by a yellow "I"; Processing Control Points, marked by a red "P"; and Output Control Points, marked by an orange "O". You may click the Pause button and take a moment to follow the controls process flowing through the illustration.

Not only do these application level control points need to be documented and tested, each legacy application may have differing Information Technology General Controls (or ITGCs) that will need to be documented and tested.

In a fully implemented ERP system environment, there is only one system, a single point of transaction entry, and a single database resulting in significantly fewer input, processing, and output control points. Furthermore, a single system would only have a single set of ITGCs.

ITGCs will be discussed in Section 3 of this module.

Please click the Forward arrow to continue.

Business process application controls include:

a) Business Process Controls
b) Interface Controls
c) The DoD Financial Management Regulations (FMR)
d) DIACAP Certification and Accreditation
e) Both A and B

Explanation

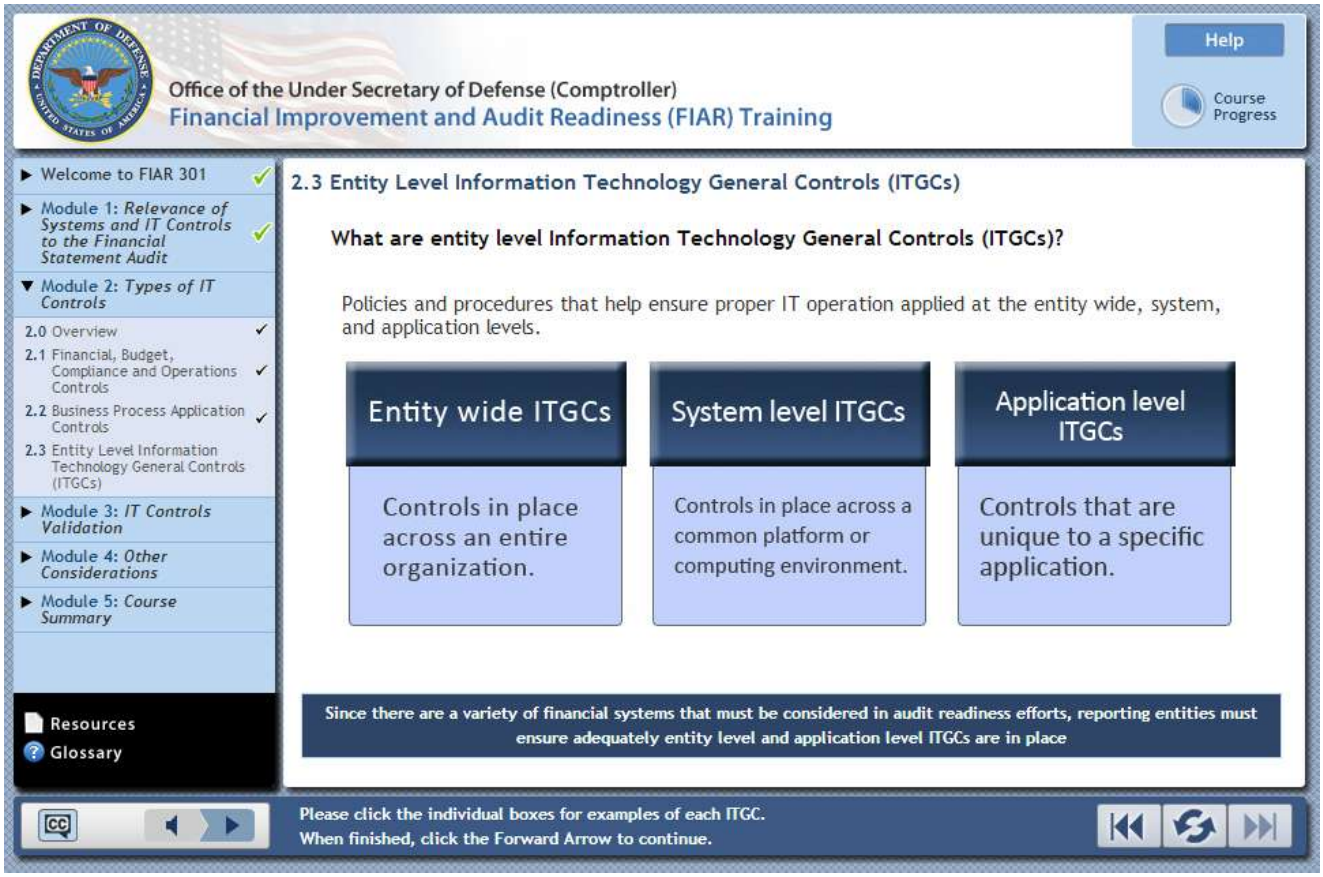
a) Incorrect. This is only one business process application control.
b) Incorrect. This is only one business process application control.
c) Incorrect. While there may be business process application controls in place that satisfy the DoD FMR, the existence of a written regulation does not by itself constitute a control.
d) Incorrect. While certain DIACAP certification and accreditation requirements align with ITGC objectives, DIACAP does not align with application control objectives related to completeness, accuracy, existence, etc.
e) Correct! Business process controls and interface controls are both business process application controls.

As legacy systems are replaced by integrated Enterprise Resource Planning (ERP) systems, the number of interfaces should be:

a) Increased
b) Reduced
c) Remain about the same

Explanation

a) Incorrect. The number of interfaces will not be increased as ERP systems replace legacy systems.
b) Correct! The number of interfaces will be reduced as ERP systems replace legacy systems.
c) Incorrect. The number of interfaces will not remain about the same as ERP systems replace legacy systems.

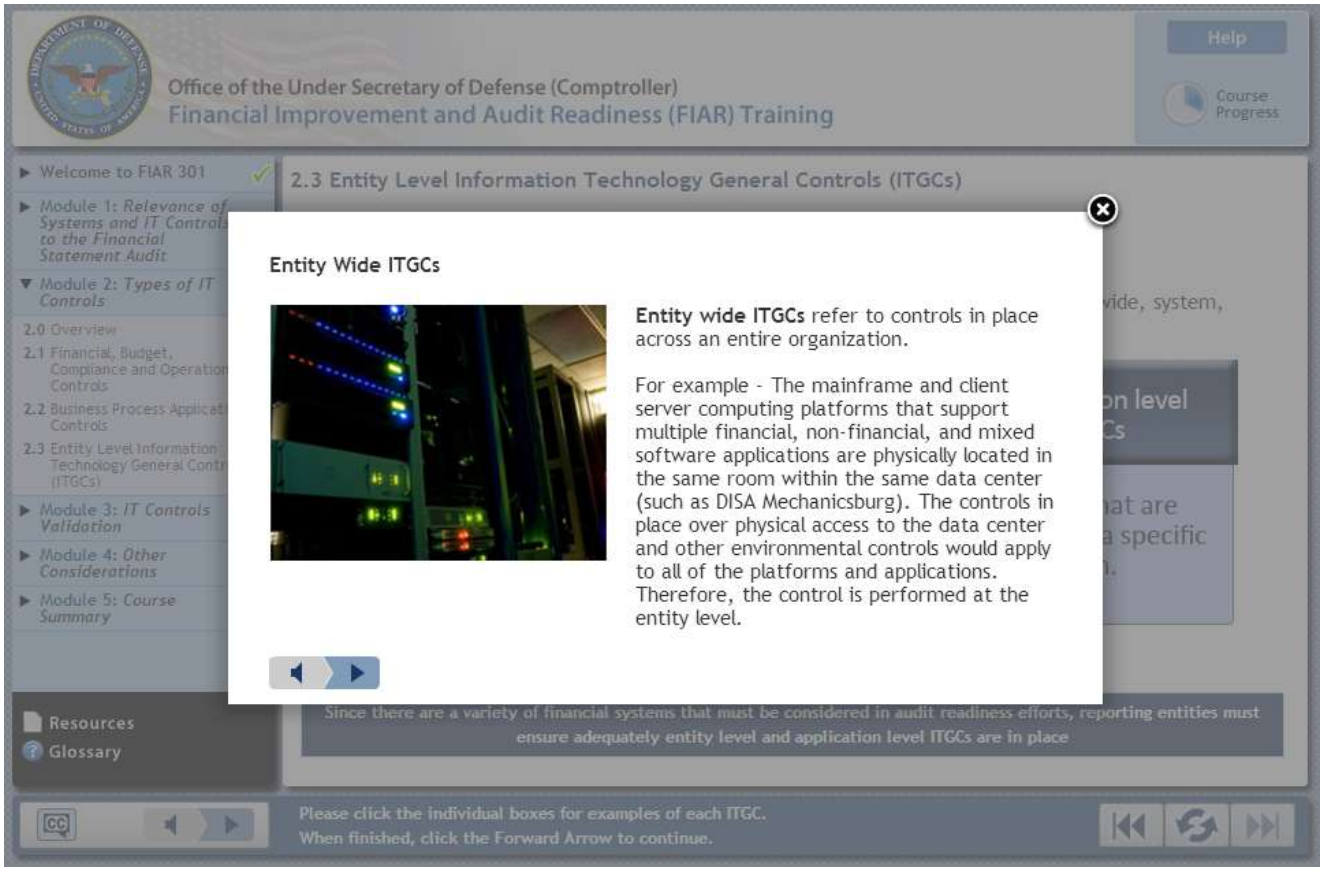


2.3 Entity Level Information Technology General Controls (ITGCs)

In this section, we will discuss IT general controls that apply to and impact all, or large groups, of applications and systems. IT general controls are applicable at the entity wide… system…and application levels. The Reporting Entity should ensure that effective IT general controls are implemented at each of these levels.

As discussed previously, IT general controls are important; they must be in place if the reporting entity wants to rely on automated controls or manual controls that use system generated information.

Please click the individual boxes for examples of each ITGC. When you are finished, please click the Forward arrow to continue.

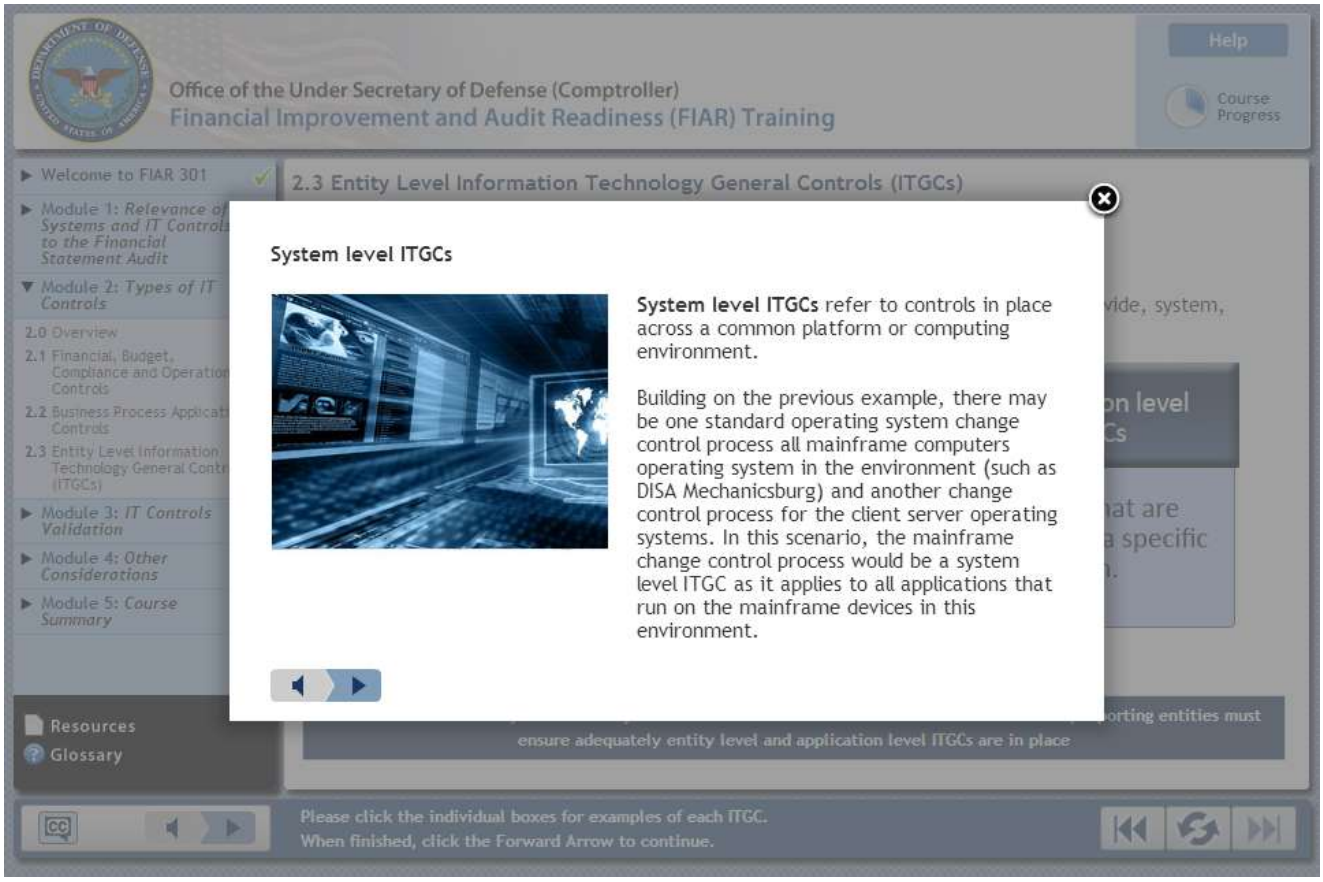


Entity wide ITGCs

Entity wide ITGCs refer to controls in place across an entire organization.

For example – The mainframe and client server computing platforms that support multiple financial, non-financial, and mixed software applications are physically located in the same room within the same data center (such as DISA Mechanicsburg). The controls in place over physical access to the data center and other environmental controls would apply to all of the platforms and applications. Therefore, the control is performed at the entity level.

Please click the "X" in the upper-right corner to close this window and continue.

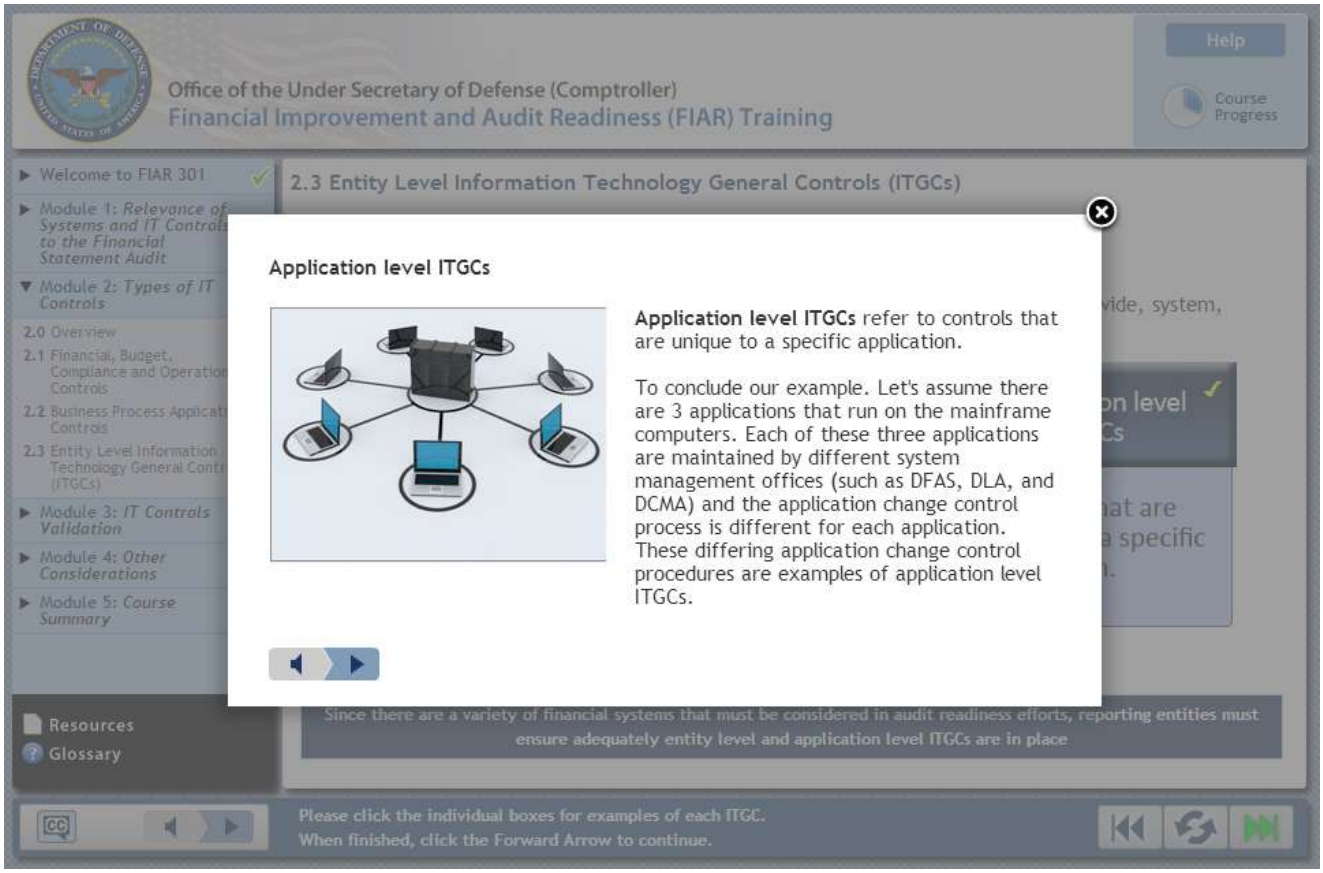


System level ITGCs

System level ITGCs refer to controls in place across a common platform or computing environment.

Building on the previous example, there may be one standard change control process for all mainframe computer operating system in the environment (such as DISA Mechanicsburg) and another change control process for the client server operating systems. In this scenario the mainframe change control process would be a system level ITGC, as it applies to all applications that run on the mainframe devices in this environment.

Please click the "X" in the upper-right corner to close this window and continue.

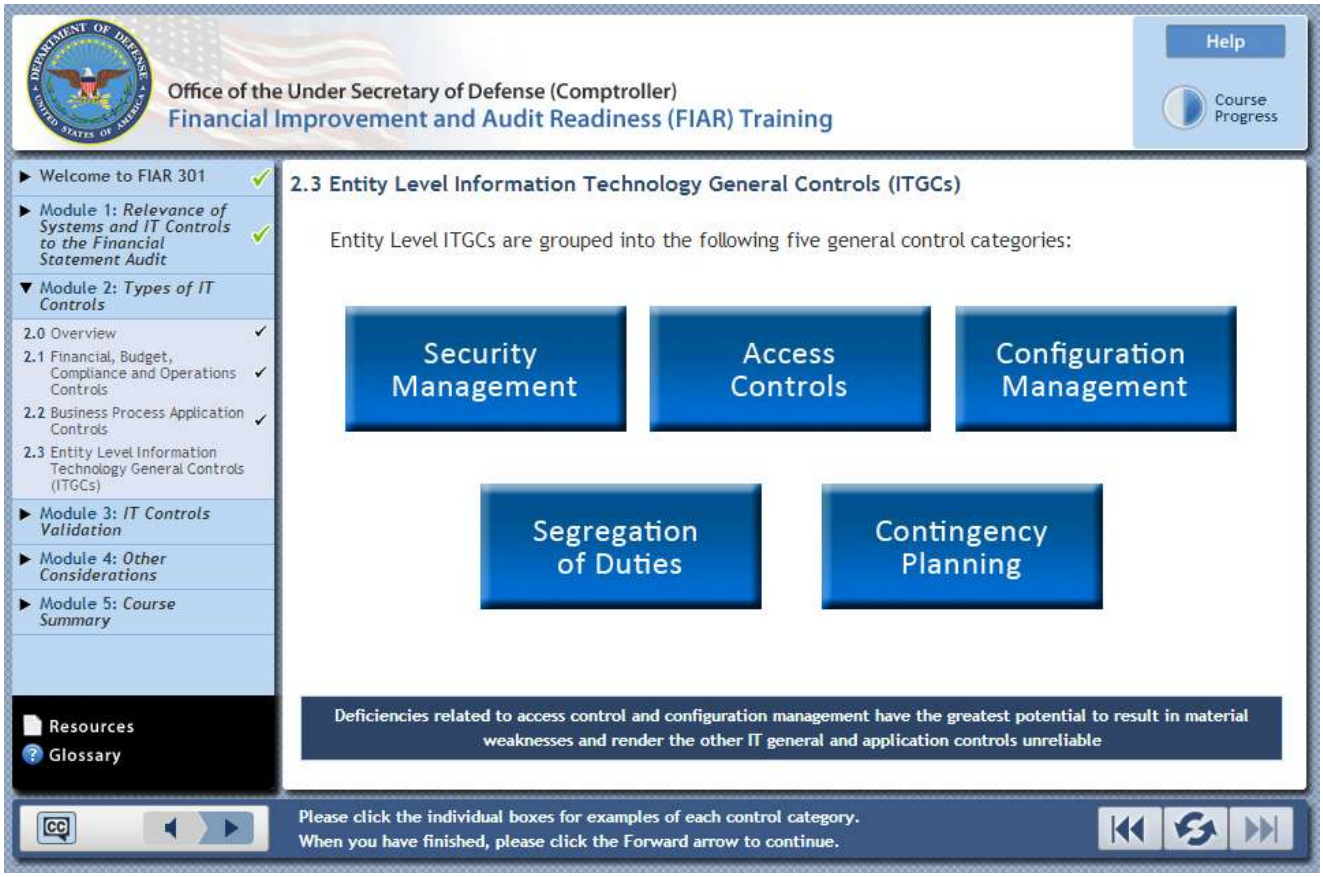


Application level ITGCs

Application level ITGCs refer to controls that are unique to a specific application.

To conclude our example, let's assume there are 3 applications that run on the mainframe computers. Each of these three applications are maintained by different system management offices (such as DFAS, DLA, and DCMA) and the application change control process is different for each application. These differing application change control procedures are examples of application level ITGCs.

Please click the "X" in the upper-right corner to close this window and continue.



2.3 Entity Level Information Technology General Controls (ITGCs)

Entity level ITGCs are grouped into the following five general control categories.

- Security Management; Access Controls; Configuration Management; Segregation of Duties; Contingency Planning

Deficiencies related to access control and configuration management have the greatest potential to result in material weaknesses and render the other IT general application controls unreliable. For example, if a developer has the access privileges needed to directly change system configuration settings, management cannot rely on system performed business process application controls or the data in reports produced by the system.

As defined and discussed in the FIAR 102 training course, there are three basic classifications of controls deficiencies that have an increasingly adverse impact on the reliability of internal controls:

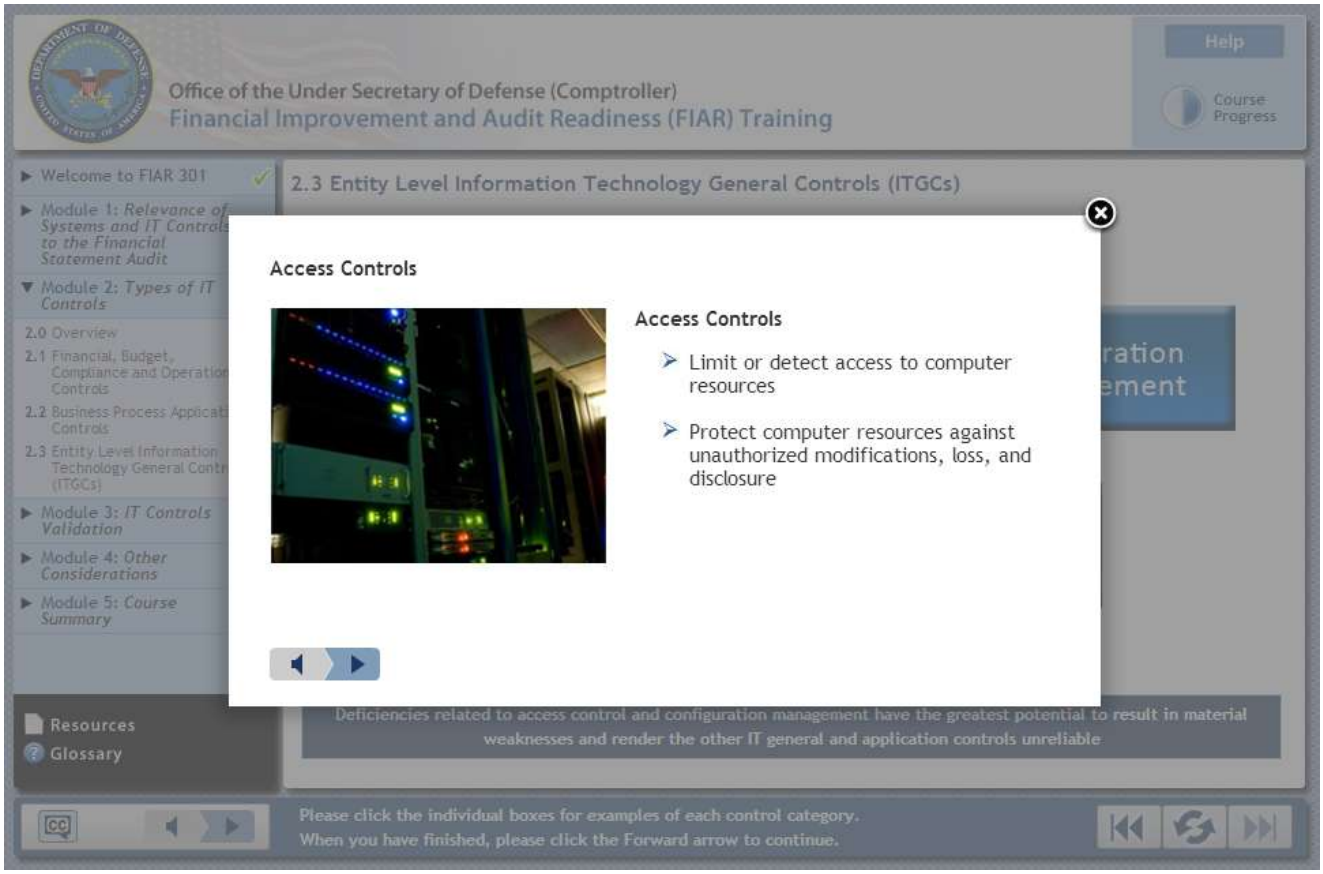
- Control Deficiency; Reportable Condition/Significant Deficiency; and Material Weakness

Please click the individual boxes for examples of each control category. When you have are finished, please click the Forward arrow to continue.

Security Management

Security Management is a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's computer-related controls.

Please click the "X" in the upper-right corner to close this window and continue.



Access Controls

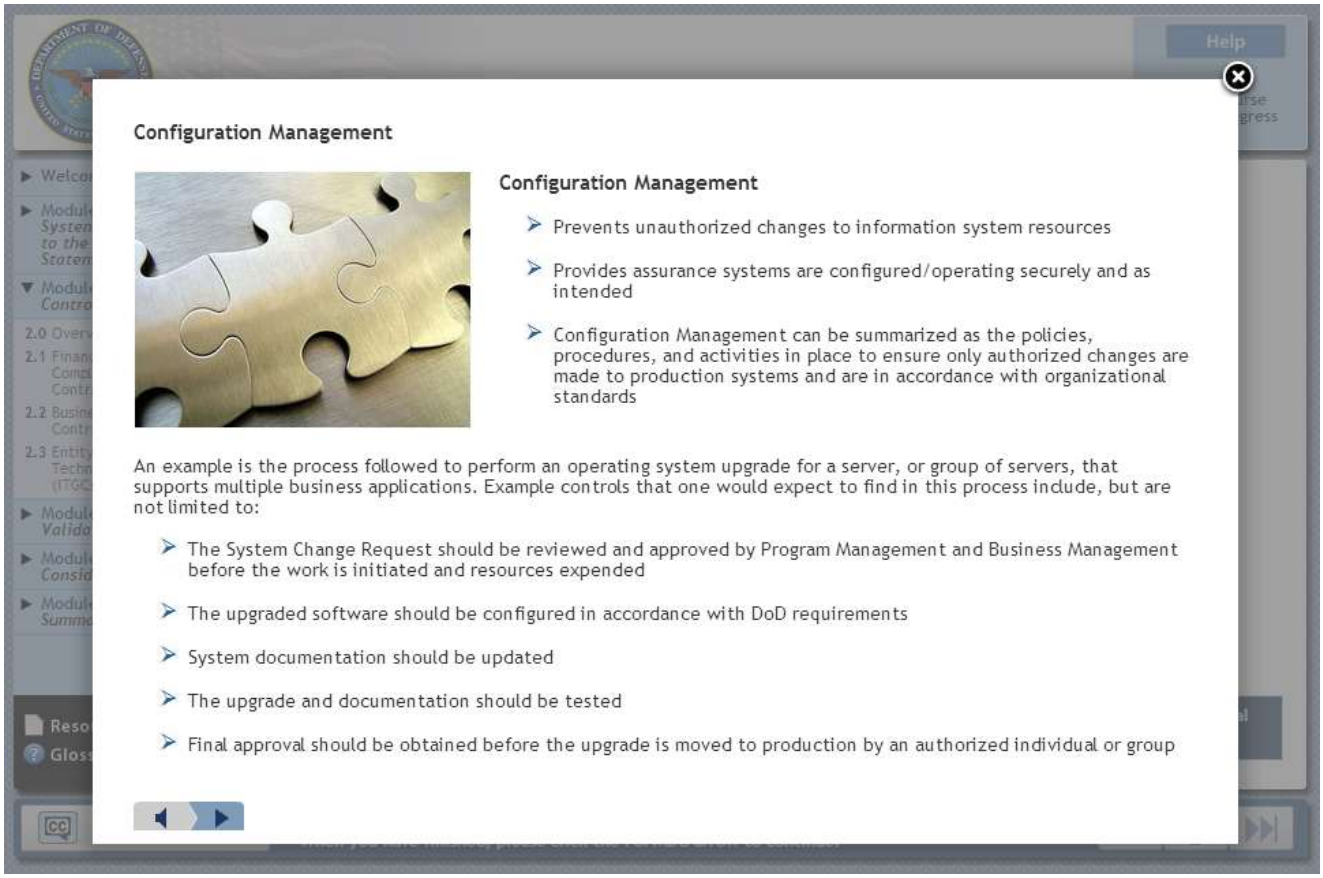
Access Controls limit or detect access to computer resources, including data, programs, equipment, and facilities, thereby protecting them against unauthorized modifications, loss, and disclosure.

Please click the “X” in the upper-right corner to close this window and continue.

Segregation of Duties

Segregation of Duties are policies, procedures, and an organizational structure to manage who can control key aspects of computer-related operations.

Please click the “X” in the upper-right corner to close this window and continue.



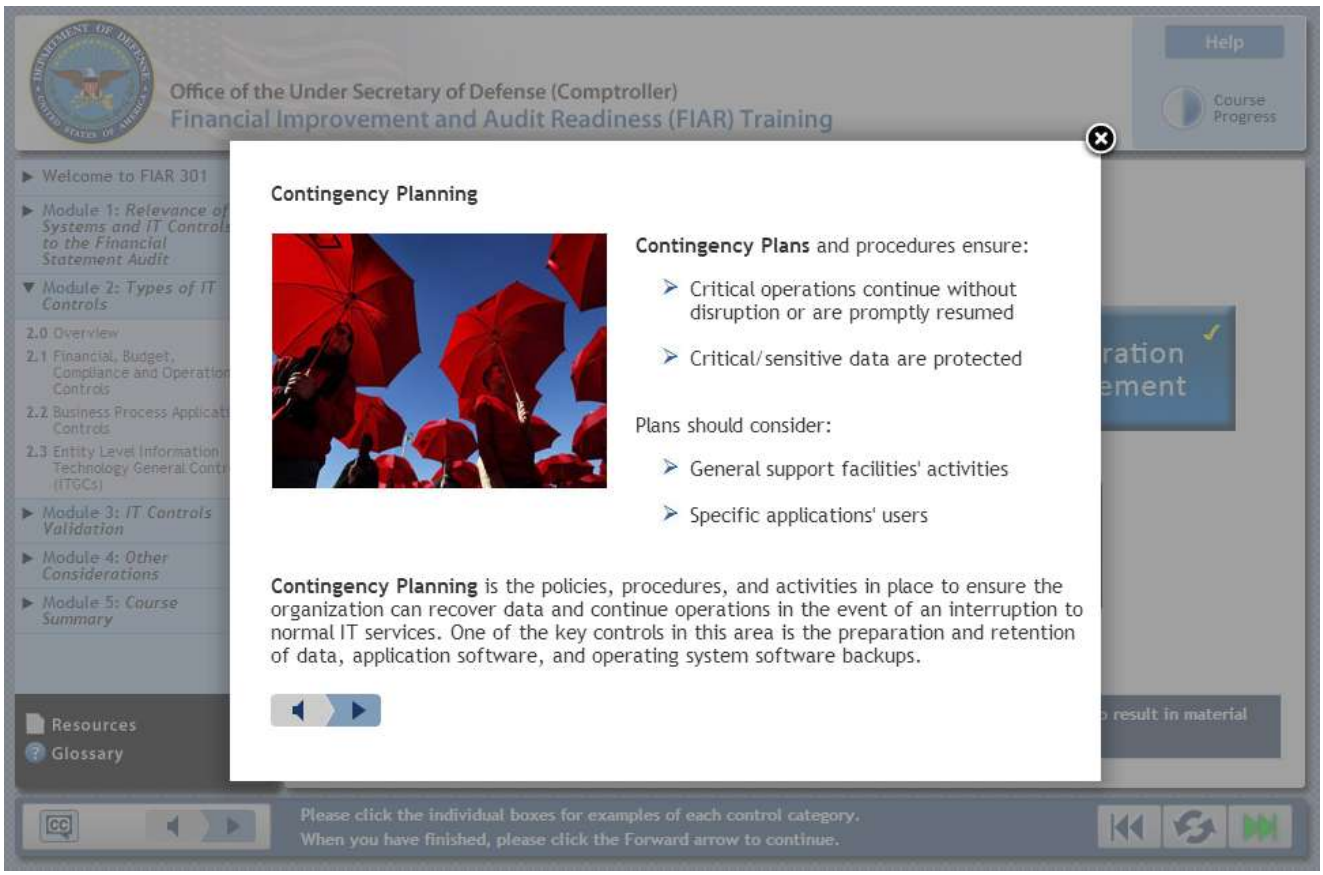
Configuration Management

Configuration Management prevents unauthorized changes to information system resources (such as software programs and hardware configurations) and provides reasonable assurance that systems are configured and operating securely and as intended.

Configuration Management can be summarized as the policies, procedures, and activities in place to ensure only authorized changes are made to production systems and these changes are in accordance with organizational standards. An example is the process followed to perform an operating system upgrade for a server, or group of servers, that supports multiple business applications. Example controls that one would expect to find in this process include, but are not limited to:

- The upgrade request (or System Change Request) should be reviewed and approved by Program Management and Business Management before the work is initiated and resources expended.
- The upgraded software should be configured in accordance with DoD requirements.
- System documentation should be updated.
- The upgrade and documentation should be tested.
- Final approval should be obtained before the upgrade is moved to production by an authorized individual or group.

Please click the “X” in the upper-right corner to close this window and continue.

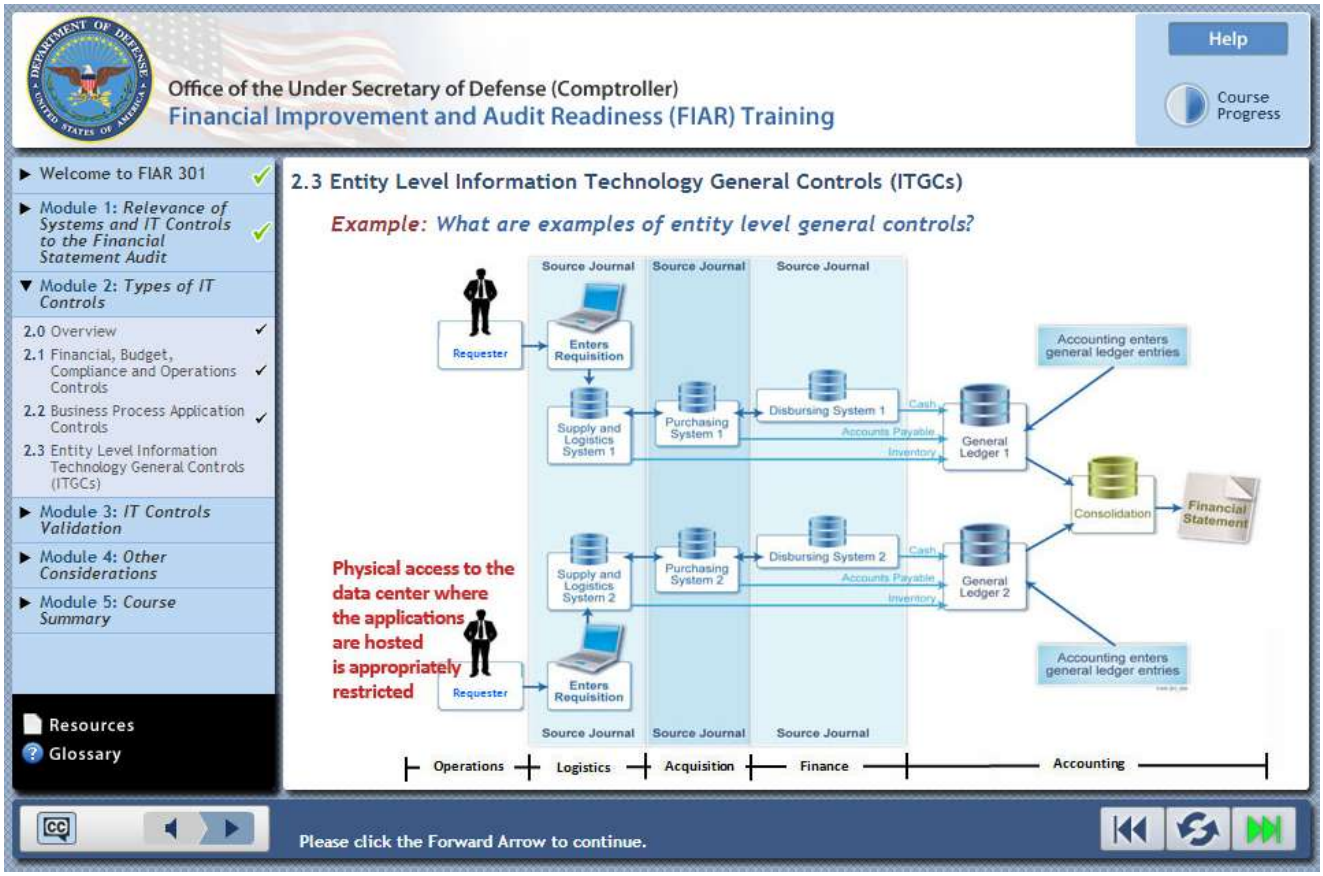


Contingency Planning

Contingency plans and procedures in place ensure that when unexpected events occur, critical operations continue without disruption or are promptly resumed, and critical and sensitive data are protected. Such plans should consider the activities performed at general support facilities, as well as those performed by users of specific applications.

Contingency Planning is the policies, procedures, and activities in place to ensure the organization can recover data and continue operations in the event of an interruption to normal IT services. One of the key controls in this area is the preparation and retention of data, application software, and operating system software backups.

Please click the "X" in the upper-right corner to close this window and continue.



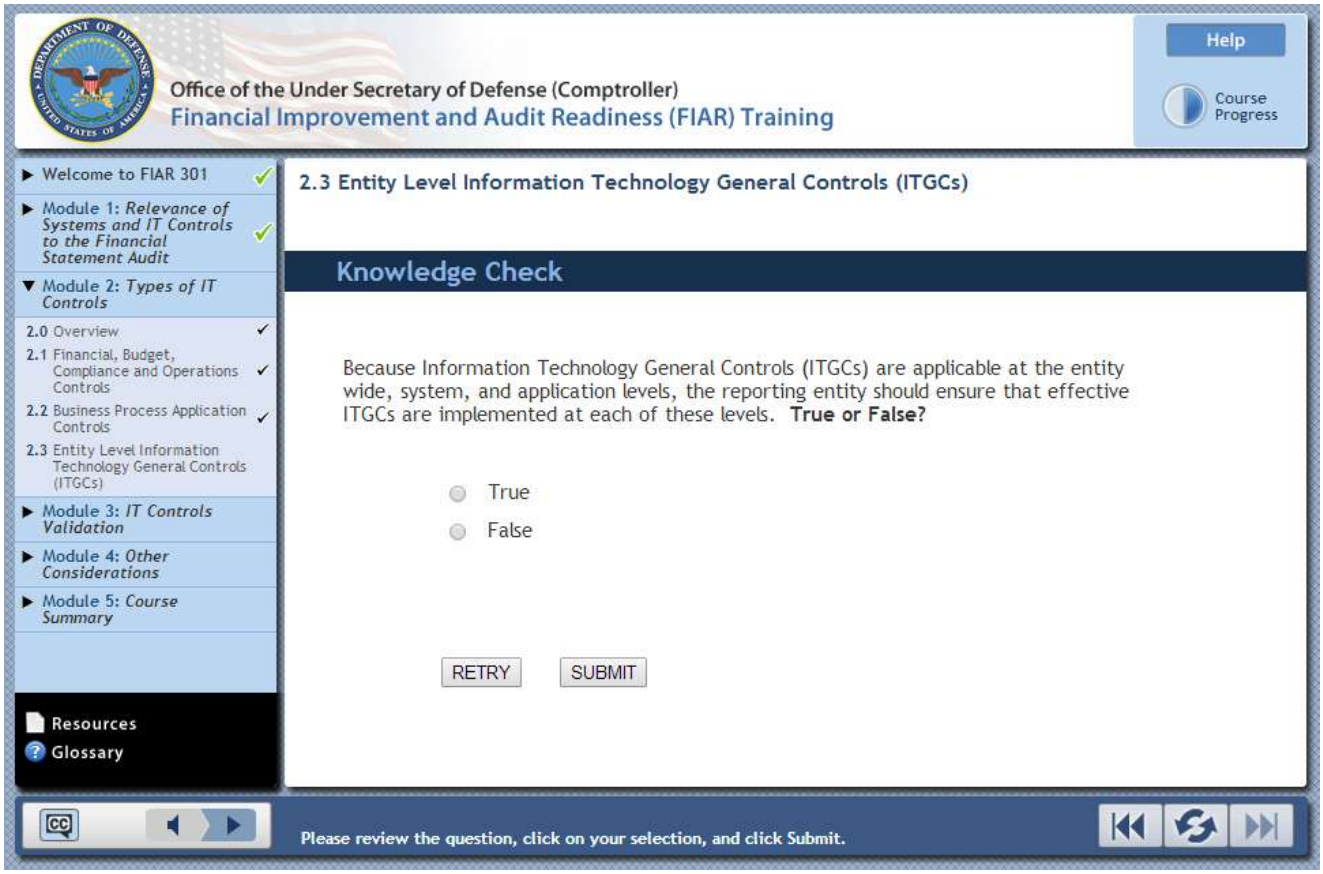
What are examples of entity level general controls?

First, let's take a look at Configuration Management. In this example, any or all configuration changes to the production operating system that impact the Supply and Logistics, Purchasing, Disbursing, General Ledger, and Consolidation applications must be approved by the organization's designated change control board.

Next, we look at Access Controls. In this example, physical access to the data center, which hosts the systems and applications, is restricted to individuals who are authorized to enter the facility.

As we mentioned earlier, material weaknesses in Configuration Management and Access Controls have the greatest potential to render the other general controls unreliable.

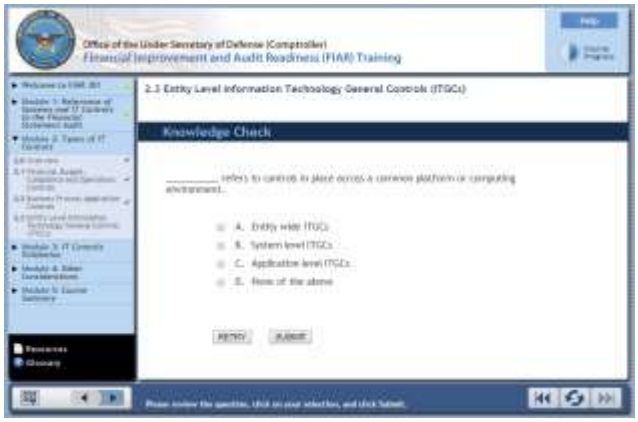
Please click the Forward arrow to continue.



Because Information Technology General Controls (ITGCs) are applicable at the entity wide, system, and application levels, the reporting entity should ensure that effective ITGCs are implemented at each of these levels. True or False?

Explanation

> ***True: Correct!*** *IT General Controls at the entity, system, and application levels can all impact the reliability of systems and therefore impact internal controls over financial reporting that rely on information produced from affected applications.*
>
> *False: Incorrect. IT General Controls at the entity, system, and application levels can all impact the reliability of systems and therefore impact internal controls over financial reporting that rely on information produced from affected applications.*



_____ refers to controls in place across a common platform or computing environment.

a) Entity wide ITGCs
b) System level ITGCs
c) Application level ITGCs
d) None of the above

Explanation

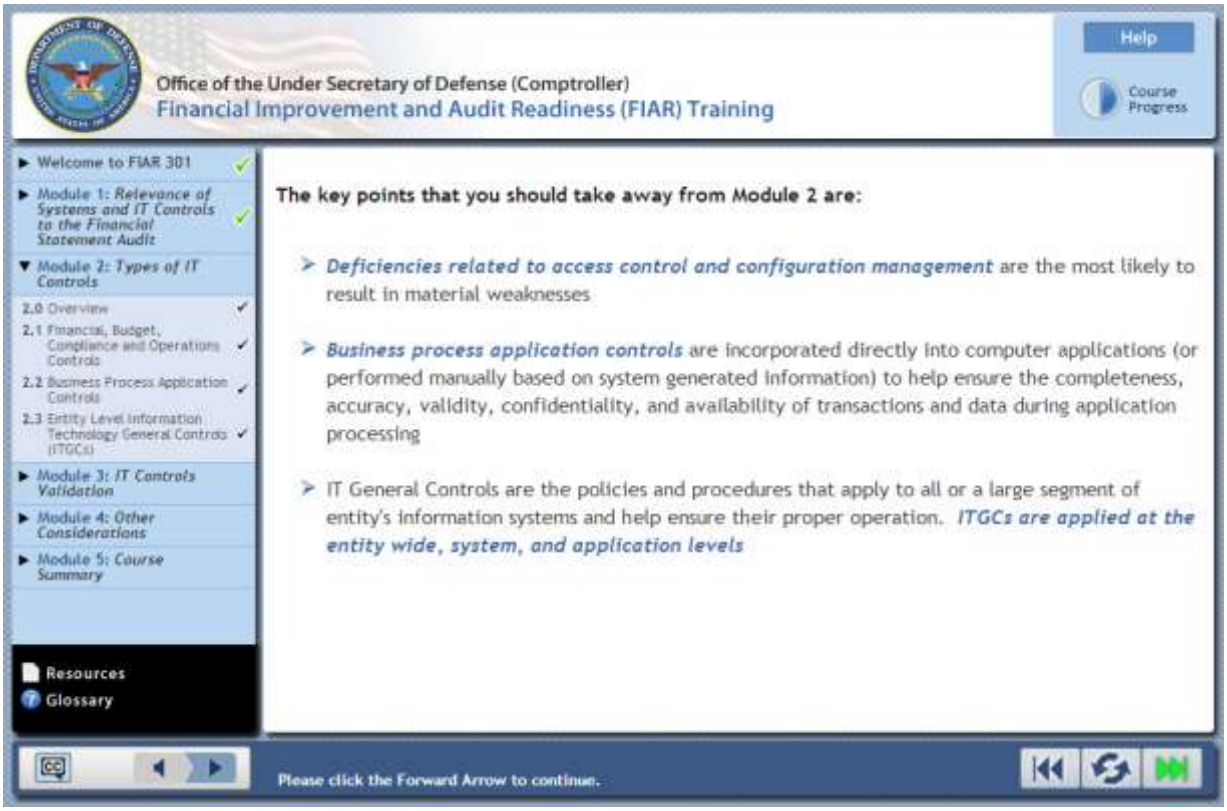
a) Incorrect. Entity wide ITGCs refer to controls in place across an entire organization.
b) Correct! System level ITGCs refer to controls in place across a common platform or computing environment.
c) Incorrect. Application level ITGCs refer to controls that are unique to a specific application.
d) Incorrect. One of the answers listed is correct.

Which of the following Information Technology General Controls (ITGCs), if found to have material weaknesses, would have the greatest potential to render the other general controls unreliable? Select only one response.

a) Security management and segregation of duties
b) Access controls and configuration management
c) Configuration management and contingency planning
d) Segregation of duties and access controls

Explanation

a) Incorrect. Although this does impose a risk of having other unreliable general controls, another answer holds a greater risk.
b) Correct! If it is determined access controls cannot be relied upon to restrict access to data and programs, it is likely that automated controls performed by applications or information provided by those applications cannot be relied upon for internal controls over financial reporting or the entity's audit readiness assertion.
c) Incorrect. Although this does impose a risk of having other unreliable general controls, another answer holds a greater risk.
d) Incorrect. Although this does impose a risk of having other unreliable general controls, another answer holds a greater risk.

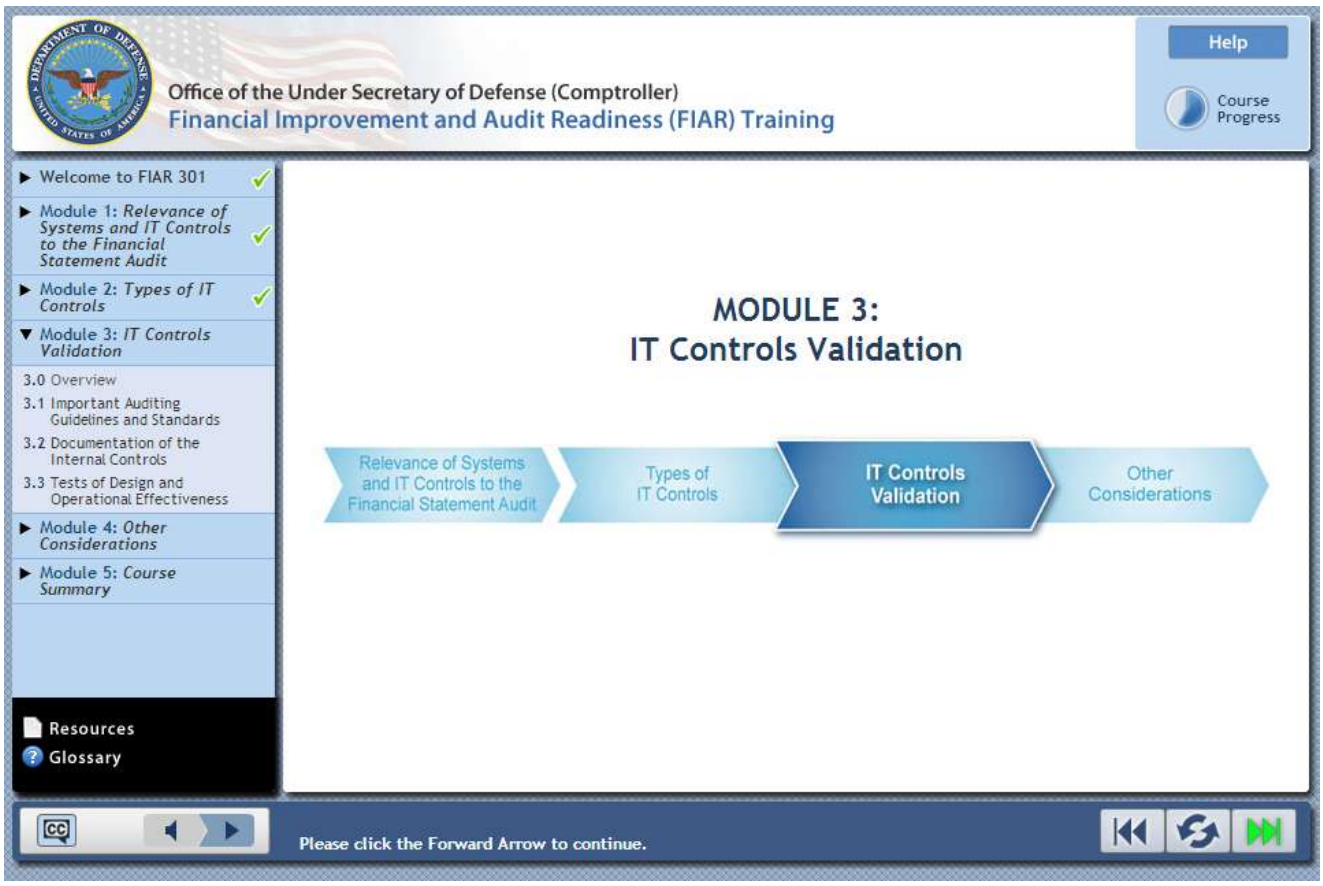


Module 2 Summary

The key points that you should take away from this Module are that:

- Deficiencies related to access control and configuration management are the most likely to result in material weaknesses.
- Business process application controls are incorporated directly into computer applications, or performed manually based on system generated information, to help ensure the completeness, accuracy, validity, confidentiality, and availability of transactions and data during application processing. Other application controls include:
    - Interface controls that are focused on the exchange of data between information systems and are primarily concerned with the completeness and accuracy of the data exchanged; and
    - Database Management System Controls that are focused on the integrity of the data that has been processed and stored by the information systems. A major area of emphasis is the ability to modify or delete processed data.
- IT General Controls (or ITGCs) are the policies and procedures that apply to all or a large segment of an entity's information systems and help ensure their proper operation. ITGCs are applied at the entity wide, system, and application levels. You may also recall that:
    - Entity wide ITGCs refer to controls in place across an entire organization;
    - System level ITGCs refer to controls in place across a common platform or computing environment; and
    - Application level ITGCs refer to controls that are unique to a specific application.

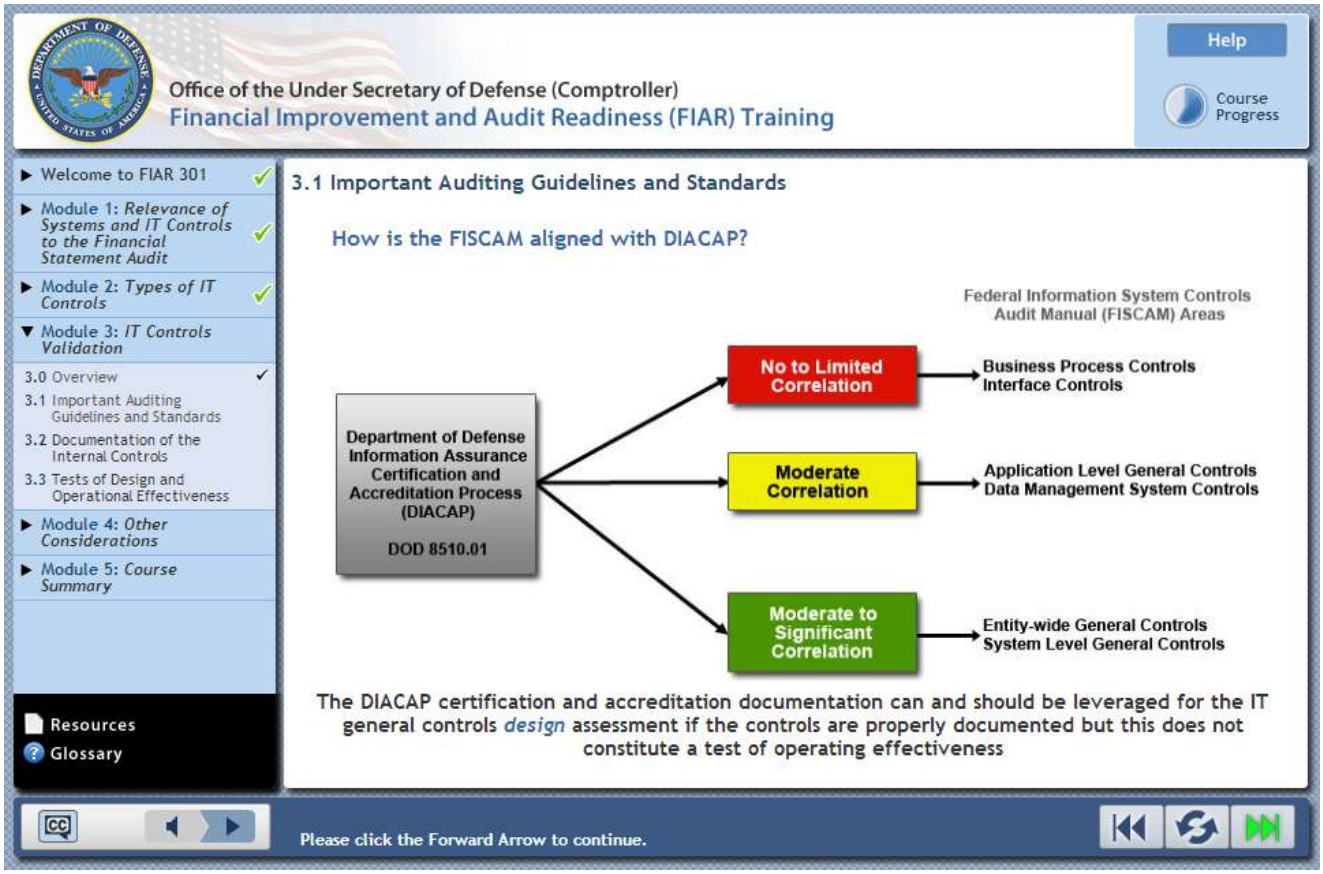
Please click the Forward arrow to continue.



Module 3 Intro: IT Controls Validation

Now we will begin Module 3. This module Introduces the guidance and standards that are relevant for evaluating IT general and applications controls; discusses the importance of documenting the design of systems and general and application controls around and within those systems; and discusses how to assess the design effectiveness of IT controls and perform tests of operating effectiveness of those controls.

Please click the Forward arrow to continue.



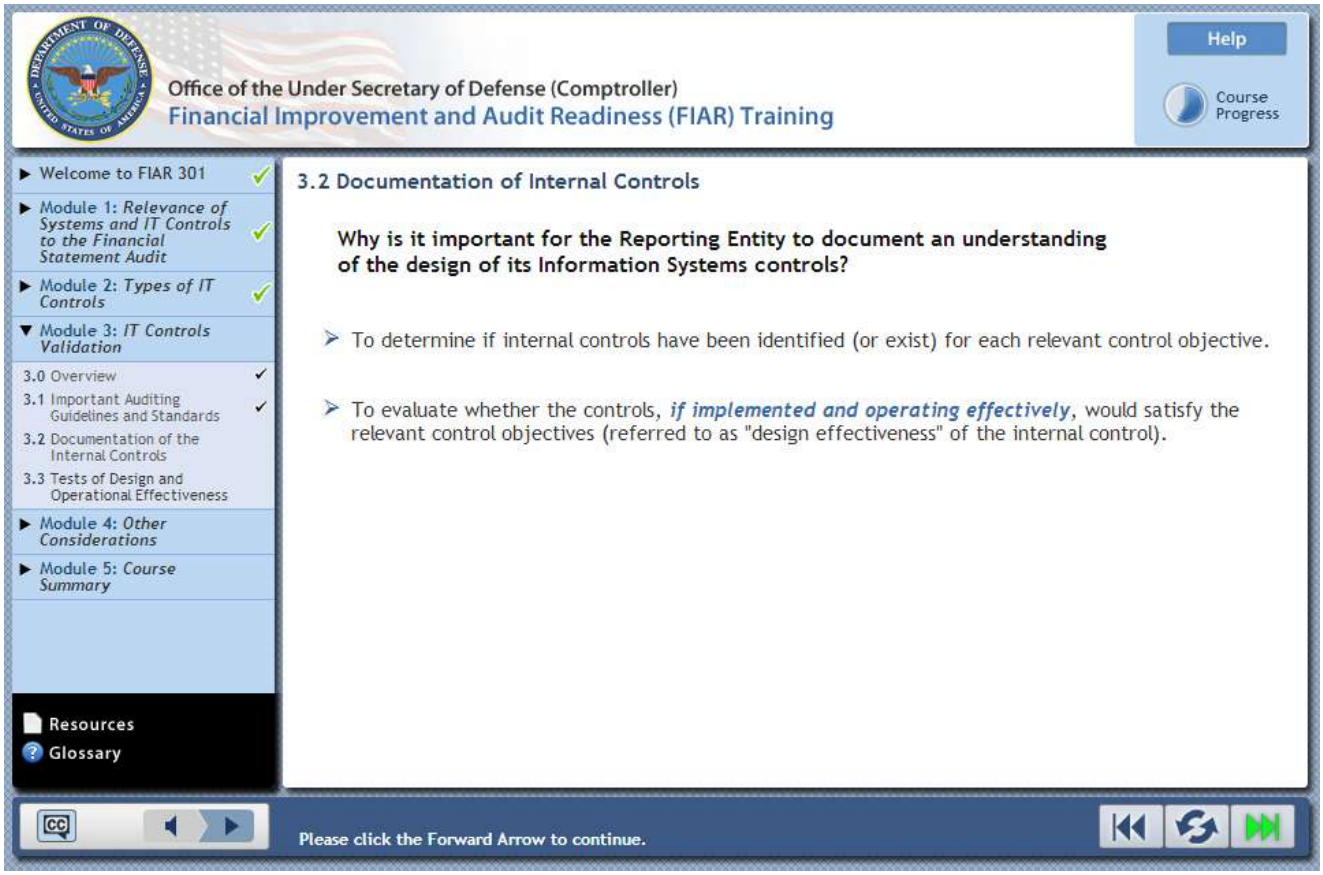
3.1 Important Auditing Guidelines and Standards

You may be familiar with the Department of Defense Information Assurance Certification and Accreditation Process (or DIACAP) that is completed before a system is connected to a DoD network, and every three years thereafter.

During the DIACAP process, a great deal of information is gathered and evaluated which may address multiple Federal Information System Controls Audit Manual (or FISCAM) IT General Control objectives and control techniques. When obtaining and documenting an understanding of the IT General Controls and assessing the design effectiveness of controls for audit readiness and/or ICOFR, the organization should leverage the DIACAP results to the extent possible.

It is important to note that the purpose of the DIACAP process differs from the audit readiness and ICOFR objectives as the DIACAP process does not entail performing tests of internal control operating effectiveness over time. Identification of business process controls are also typically outside the scope of DIACAP.

Please click the Forward arrow to continue.



3.2 Documentation of Internal Controls

It is important for the Reporting Entity to document an understanding of IT general and application controls for two primary reasons:

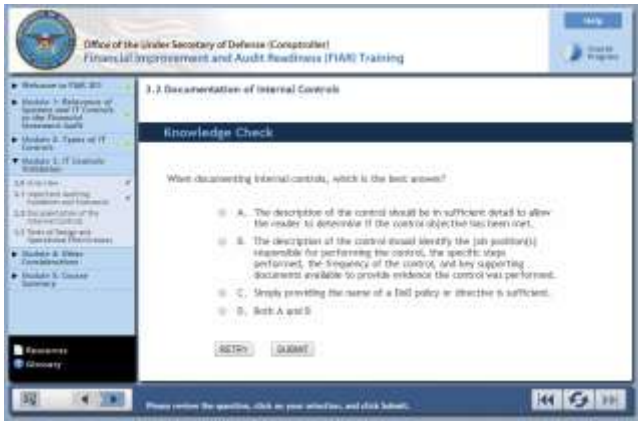
- The first is simply to determine if internal controls have been identified, or exist, for each relevant control objective.
- The second is to evaluate whether the controls, if implemented and operating effectively, would satisfy the relevant control objectives. This is often referred to as assessing the “design effectiveness” of the internal control.

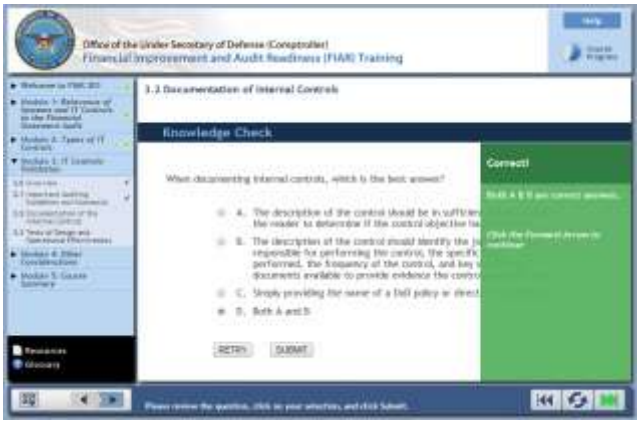
This includes documenting the design of the entity’s information system controls related to:

- The Organization; Staffing; Responsibilities; Authorities; and Resources of the Entity’s Security Management Function.

The reporting entity should obtain and document an understanding of the design of its information systems controls to the extent necessary to tentatively conclude whether these controls are likely to be effective. Best practice is to document the who, what, where, when, and how often for the controls.

Please click the Forward arrow to continue.



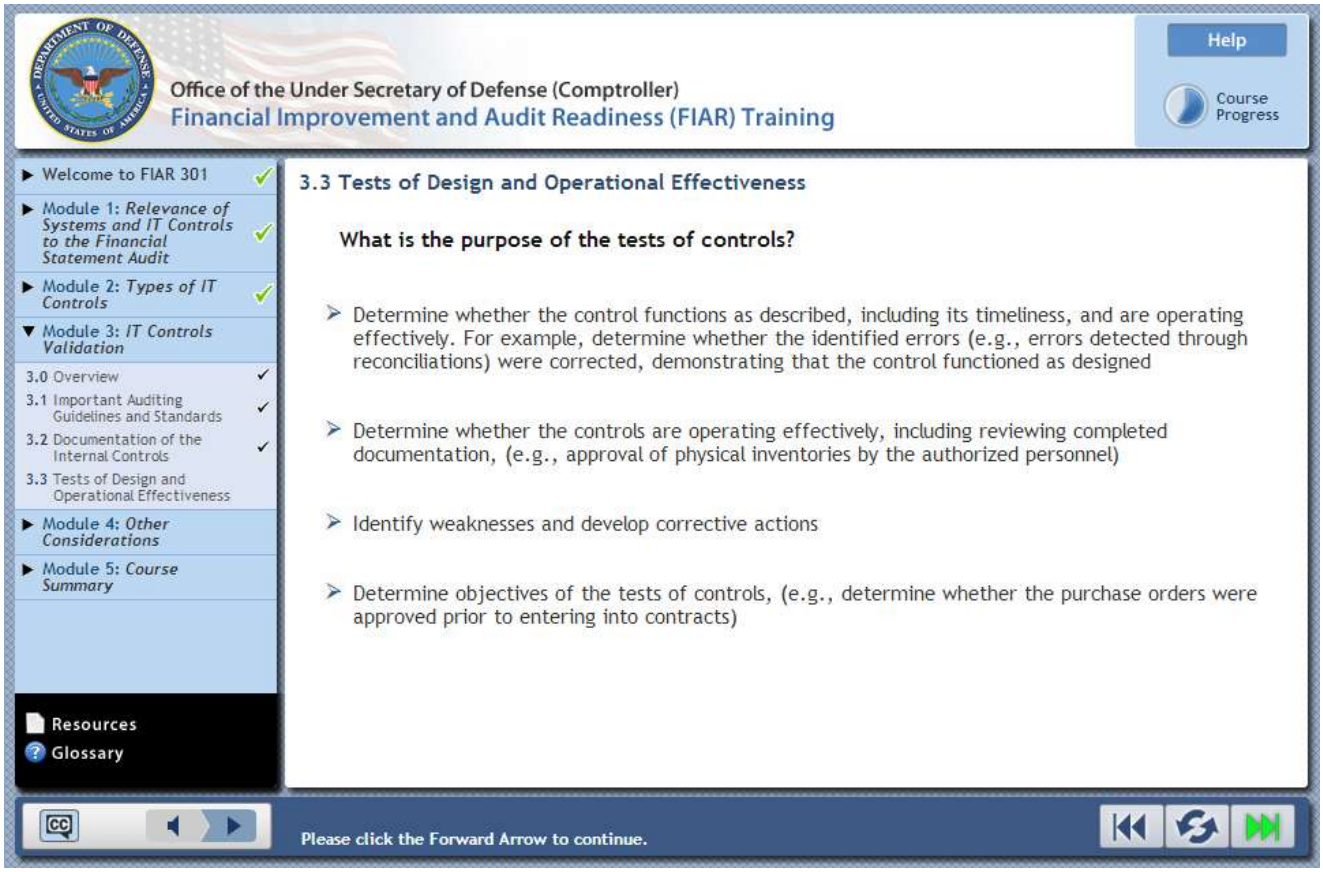


When documenting internal controls, which is the best answer?

a) The description of the control should be in sufficient detail to allow the reader to determine if the control objective has been met.
b) The description of the control should identify the job position(s) responsible for performing the control, the specific steps performed, the frequency of the control, and key supporting documents available to provide evidence the control was performed.
c) Simply providing the name of a DoD policy or directive is sufficient.
d) Both A and B

Explanation

a) Incorrect. Although answer should be documented, it is only part of the correct answer.
b) Incorrect. Although answer should be documented, it is only part of the correct answer.
c) Incorrect. Simply identifying the name of a DoD policy or directive does not give the reader/auditor enough information to determine if the control objective has been met. It also does not provide any information regarding the key supporting documentation available for inspection during testing.
d) Correct! Both A & B are correct answers.



3.3 Tests of Design and Operational Effectiveness

Before we discuss how to perform the tests of controls, let's discuss its purpose.

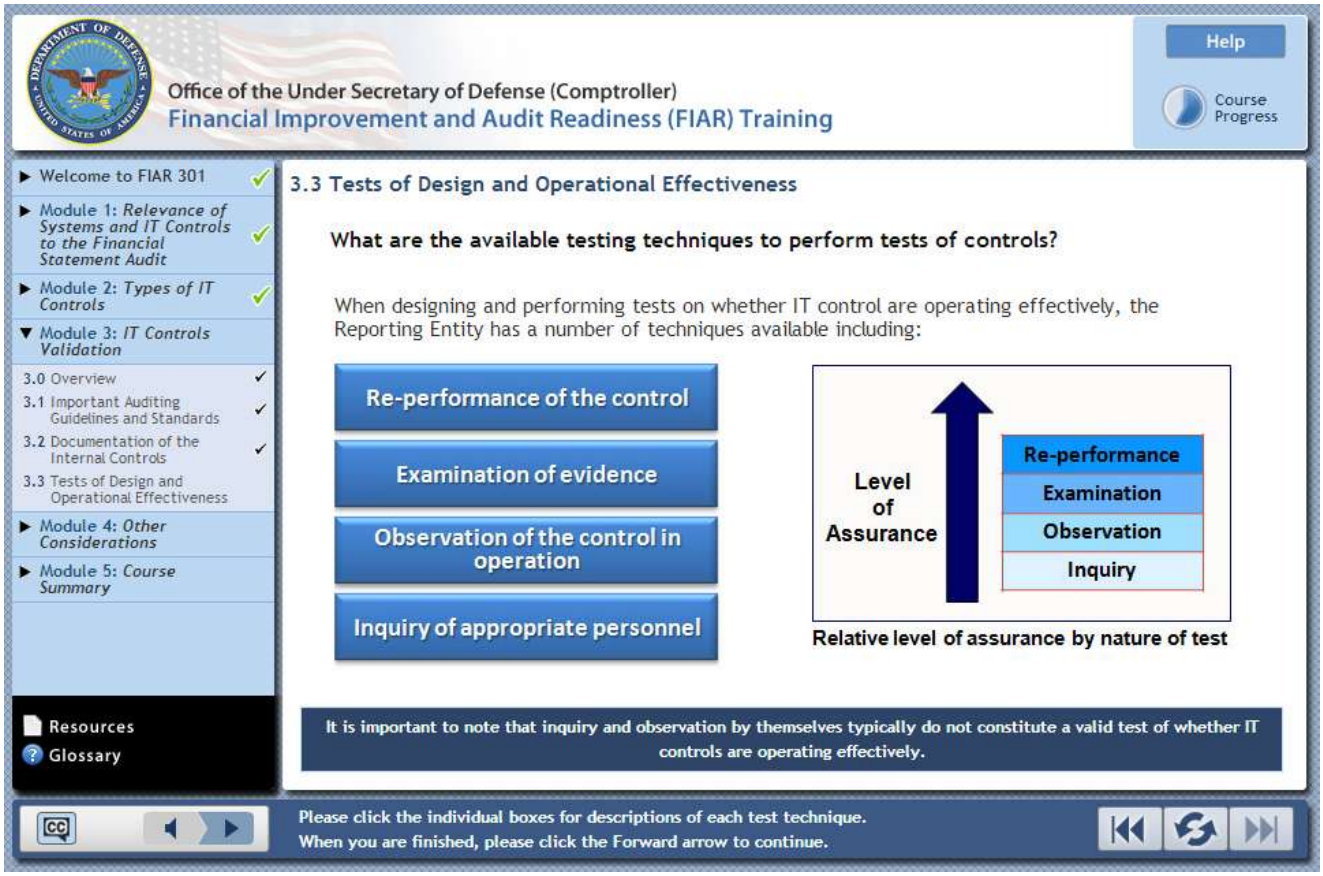
The purpose of the test of control is to determine whether the controls function as described, including its timeliness, and are operating effectively. This determination is made by reviewing completed documentation demonstrating performance of control, such approval of physical inventories by authorized personnel.

Also, the purpose of the test of controls is to identify weaknesses in controls and develop corrective actions to remediate the weaknesses. For example, the reporting entity may have implemented a control requiring approval of monthly reconciliation of inventory by the branch chief. However, the branch chief may not actually perform the review or document his/her review. Through the test of control, this weakness related to lack of review and documentation can be identified and remediated through corrective actions.

Now that you understand the purpose of the tests of controls, let's discuss the process for designing and performing the test of controls.

As a reminder before beginning the test of controls, reporting entities need to assess the design of the controls and identify the controls that are designed effectively. This should be completed in conjunction with the Controls Assessment, which is part of Activity 1.3.3. The reporting entity should determine the objective (or purpose) of the test of control. For example, if the objective of the test of control is to determine whether the controls surrounding the completeness assertion are operating effectively, such as periodic physical inventory, then the reporting entity should test controls that are related to the physical inventory process, rather than the controls related to the valuation of the inventory. The key to successful completion of the test of control is dependent upon identifying the test objective and then designing the test to meet those objectives.

Please click the Forward arrow to continue.



What are the available test techniques?

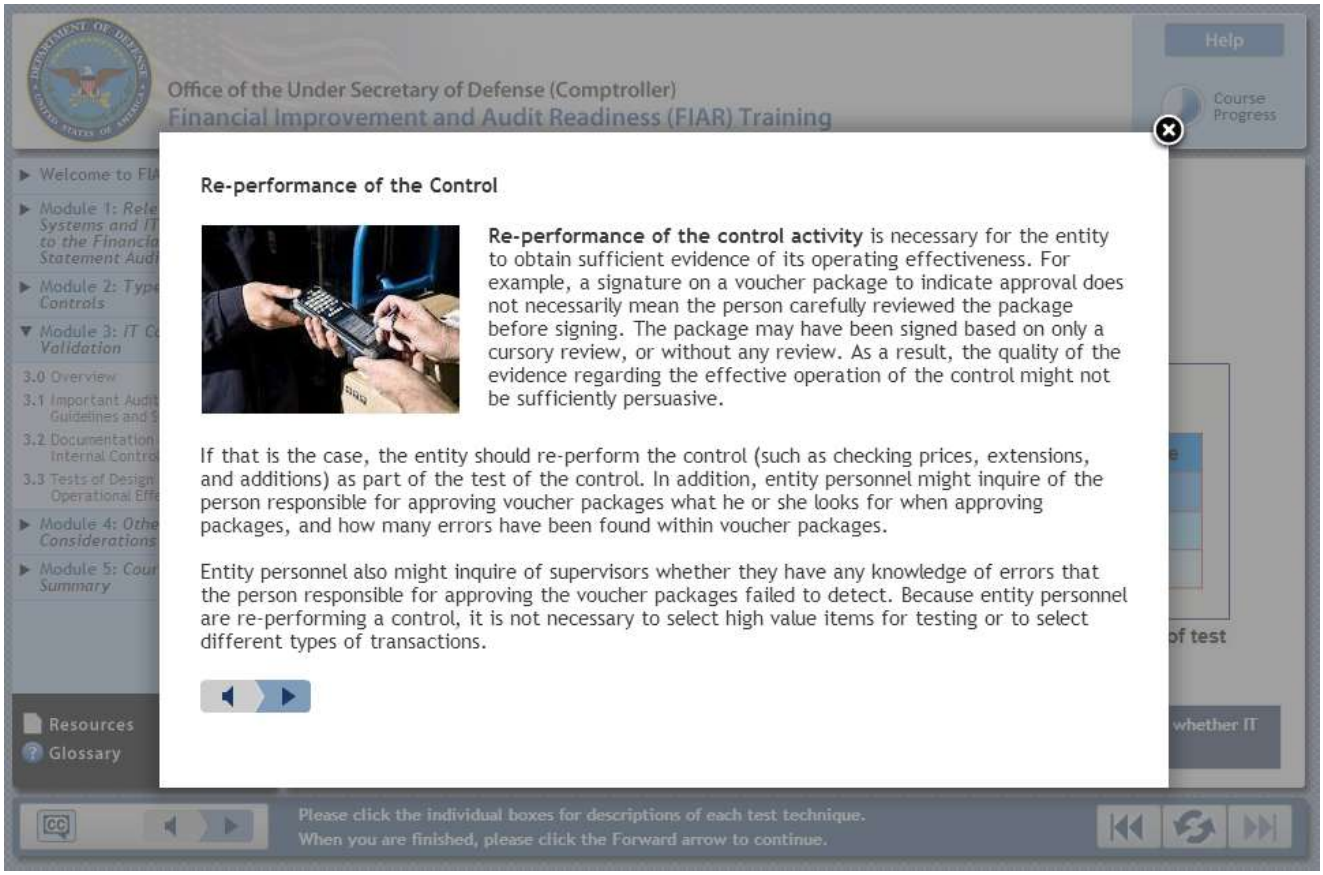
When designing and performing tests of operating effectiveness of IT controls, the reporting entity has a number of possible testing techniques. They include:

- Re-performance of the control;
- Examination of evidence;
- Observation of the control in operation; and,
- Inquiry of appropriate personnel

The techniques are listed in order of relative ability to provide assurance, as illustrated in the graphic. Those listed at or near the top typically provide the highest level of assurance that the control has been operating effectively over time, while those listed closer to the bottom provide lower levels of assurance. It is important to note that no one testing technique by itself can provide strong assurance that controls are operating effectively; instead, tests of controls are performed using a combination of one or more of these testing techniques.

Also, tests of inquiry and observation by themselves do not constitute valid tests to conclude on the operating effectiveness of IT controls. However, they can be very useful in obtaining an understanding of the operation of controls and are usually performed during the walkthrough process described in FIAR 102. Additional detail on testing of internal controls can be found in the FIAR 102 course.

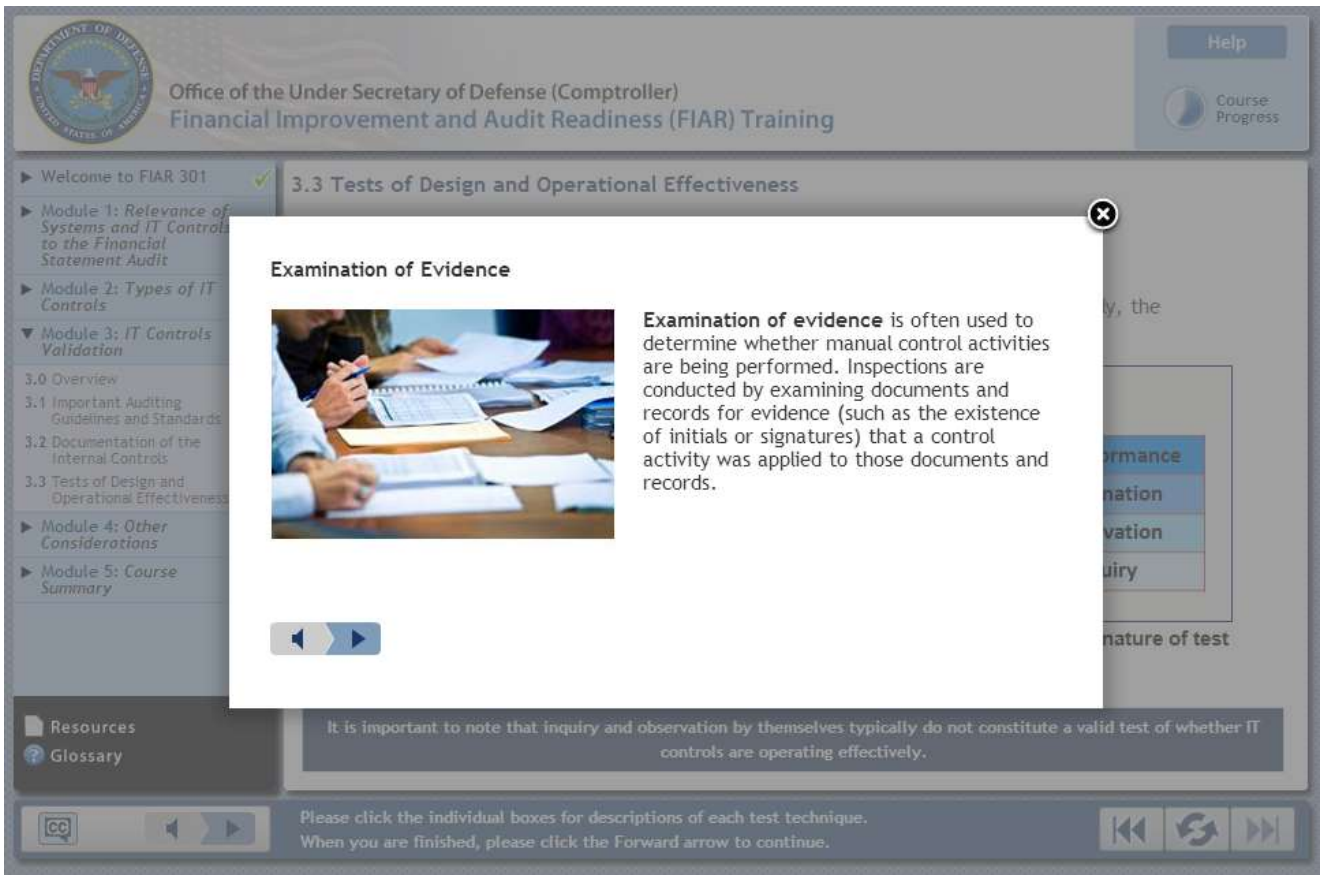
Please click the individual boxes for descriptions of each test technique. When you are finished, please click the Forward arrow to continue.



Re-performance

Re-performance of the control activity is necessary for the entity to obtain sufficient evidence of its operating effectiveness. For example, a signature on a voucher package to indicate approval does not necessarily mean the person carefully reviewed the package before signing. The package may have been signed based on only a cursory review, or without any review. As a result, the quality of the evidence regarding the effective operation of the control might not be sufficiently persuasive. If that is the case, the entity should re-perform the control (such as checking prices, extensions, and additions) as part of the test of the control. In addition, entity personnel might inquire of the person responsible for approving voucher packages what he or she looks for when approving packages, and how many errors have been found within voucher packages. Entity personnel also might inquire of supervisors whether they have any knowledge of errors that the person responsible for approving the voucher packages failed to detect. Because entity personnel are re-performing a control, it is not necessary to select high value items for testing or to select different types of transactions.

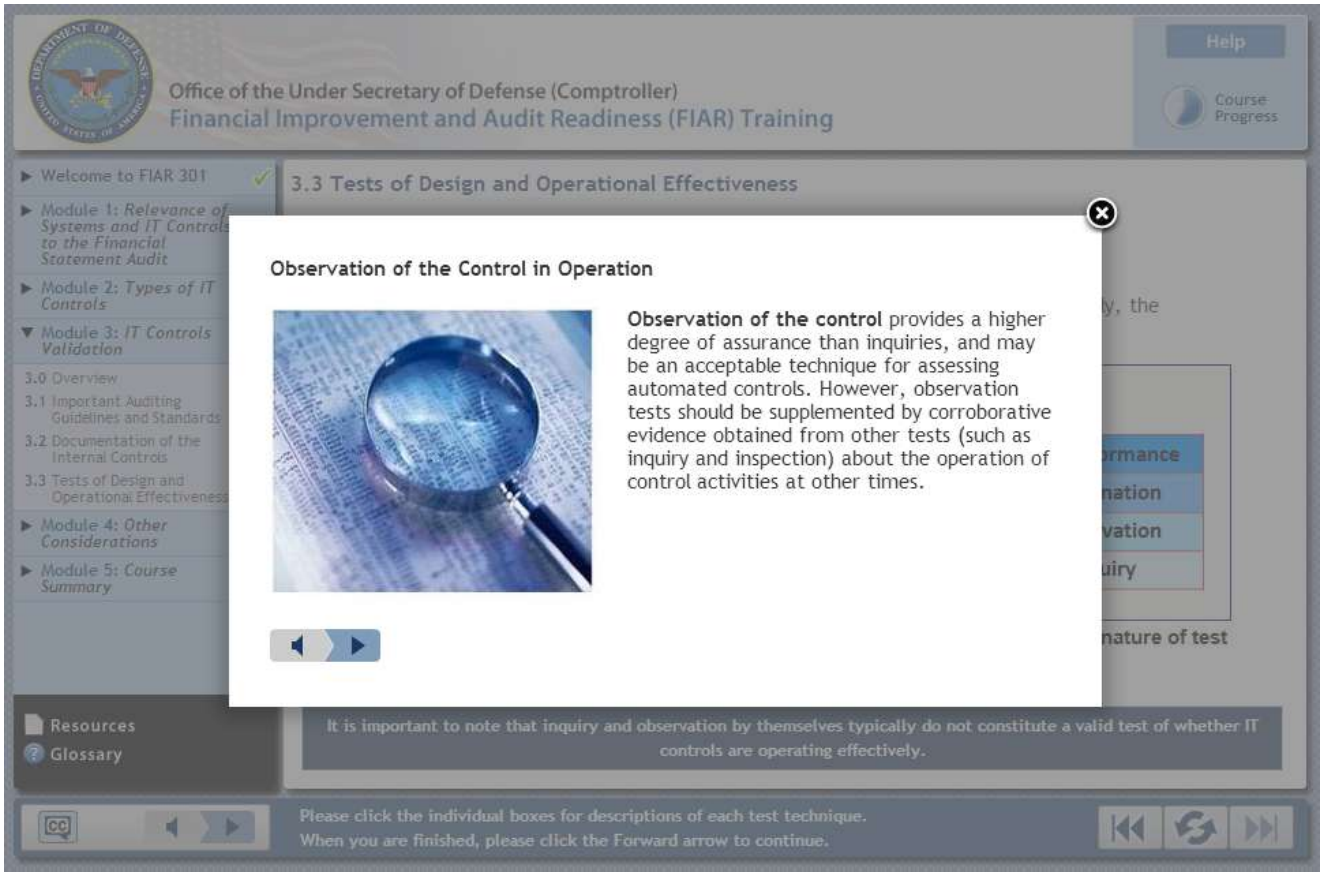
Please click the "X" in the upper-right corner to close this window and continue.



Examination

Examination of evidence is often used to determine whether manual control activities are being performed. Inspections are conducted by examining documents and records for evidence (such as the existence of initials or signatures) that a control activity was applied to those documents and records.

Please click the "X" in the upper-right corner to close this window and continue.



Observation

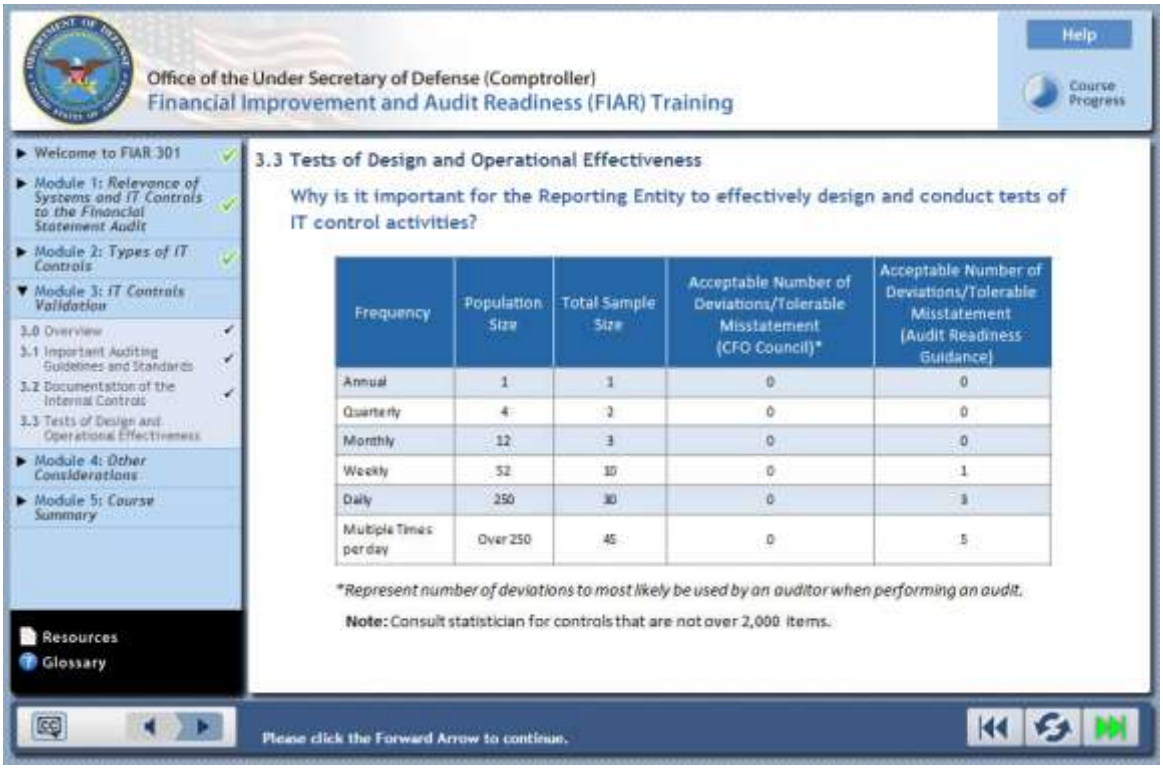
Observation of the control provides a higher degree of assurance than inquiries, and may be an acceptable technique for assessing automated controls. However, observation tests should be supplemented by corroborative evidence obtained from other tests (such as inquiry and inspection) about the operation of control activities at other times.

Please click the "X" in the upper-right corner to close this window and continue.

Inquiry

Inquiry tests are conducted by making either oral or written inquiries of entity personnel involved in the execution of specific control activities to determine what they do or how they perform a specific control activity. The inquiries are typically open-ended. Evidence obtained through inquiry is the least reliable evidence and should be corroborated through other types of control tests (such as observation or inspection). Inquiry regarding a control's effectiveness does not, by itself, provide sufficient evidence about whether a control is operating effectively.

Please click the "X" in the upper-right corner to close this window and continue.



3.3 Tests of Design and Operational Effectiveness

When performing tests of operating effectiveness, it is important to select an adequate number of sample items to test for the given audit/assertion period.

In determining how extensively a key control should be tested (such as sample size or type of test performed), management should consider the complexity of the key control as well as the frequency with which the control is performed. A highly complex control that is performed daily should be tested more often than a less complex control performed annually.

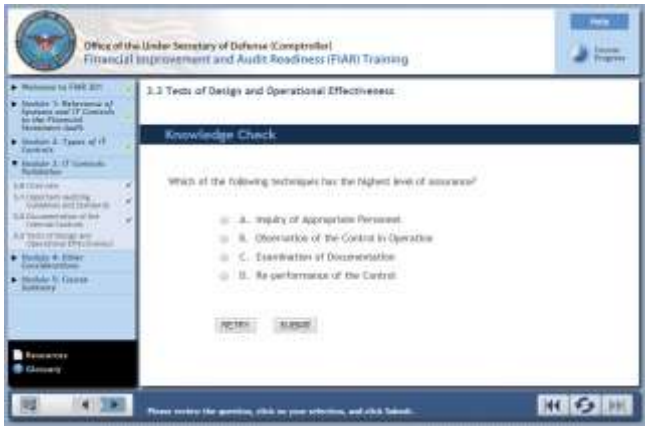
The CFO Council, Implementation Guide for OMB Circular A-123, Appendix A, provides guidance for determining sample sizes, based on the frequency of a control activity, that will support a conclusion that a manual control is operating effectively. This table details the CFO Council's guidance along with an acceptable number of deviations that reporting entities can use only for audit readiness purposes (found in the last column). The Department has determined that for certain sample sizes, a larger number of deviations from that accepted by the CFO Council's guidance will be acceptable for audit readiness purposes. However, Management must accept the implications of sampling risk and understand that testing under a financial statement audit will be more rigorous and allow fewer deviations. Entities must document the justification of the sample size used for testing if it differs from the guidance.

In addition, whether the control is manual or automated should also be considered, as sample sizes for automated controls will usually be smaller than those for manual controls, provided that the IT general controls have been found to be operating effectively. Ultimately, management should use its best judgment to determine how extensively a key control will be tested. However, the rationale for the judgment should be documented.

An example of annual controls could include closing the General Ledger posting period (which should only happen once per year). In contrast, requests for system access privileges are performed many times every day.

Please note: The use of sampling during testing of internal controls is covered in additional detail in the FIAR 102 course.

Please click the Forward arrow to continue.

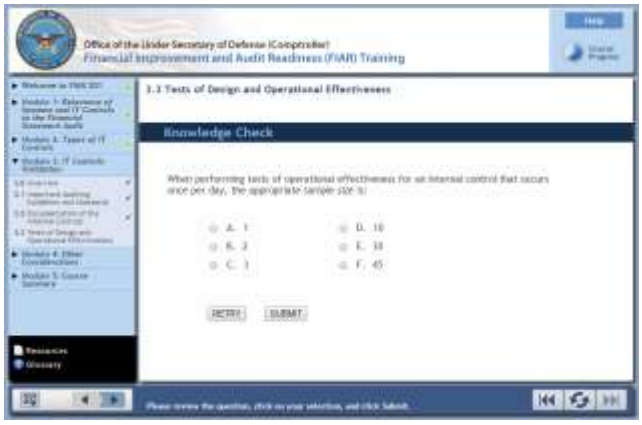


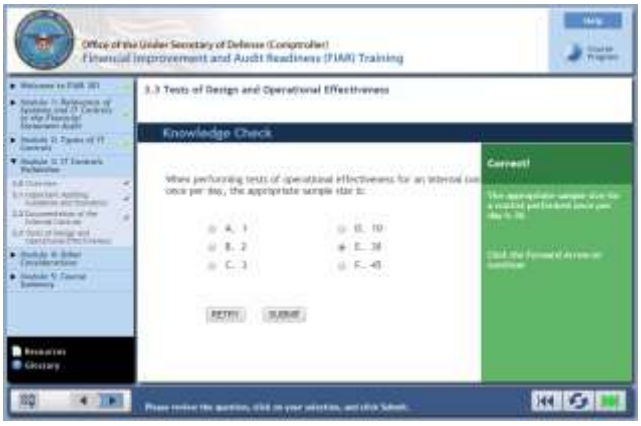
Which of the following techniques has the highest level of assurance?

a) Inquiry of Appropriate Personnel
b) Observation of the Control in Operation
c) Examination of Documentation
d) Re-performance of the Control

Explanation

a) Incorrect. Inquiry of Appropriate Personnel has the lowest level assurance.
b) Incorrect. Observation of the Control in Operation has a medium level of assurance.
c) Incorrect. Inspection of Documentation has a medium level of assurance.
d) Correct! Re-performance of the Control provides the highest level of assurance.



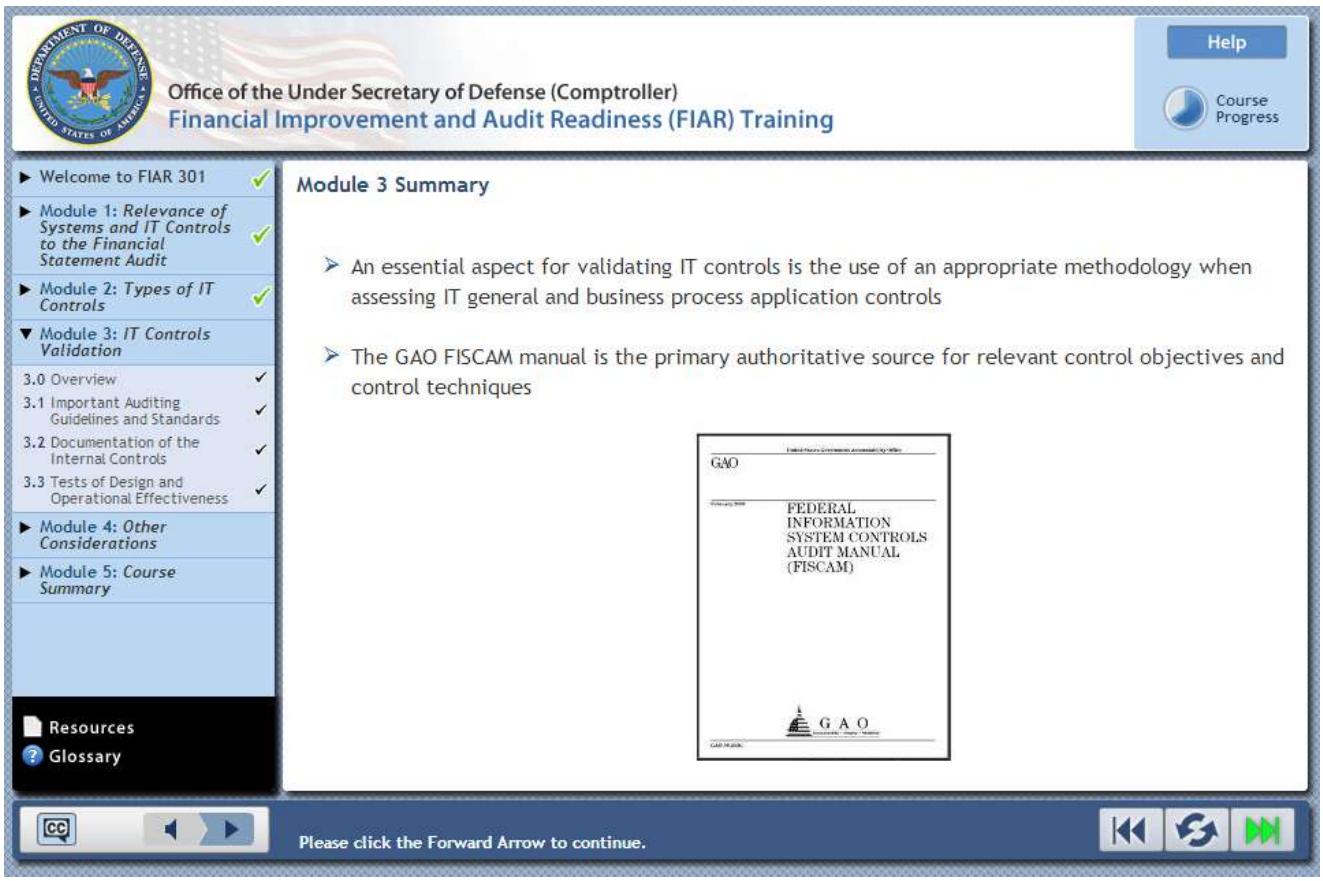


When performing tests of operational effectiveness for an internal control that occurs once per day, the appropriate sample size is:

a) 1
b) 2
c) 3
d) 10
e) 30
f) 45

Explanation

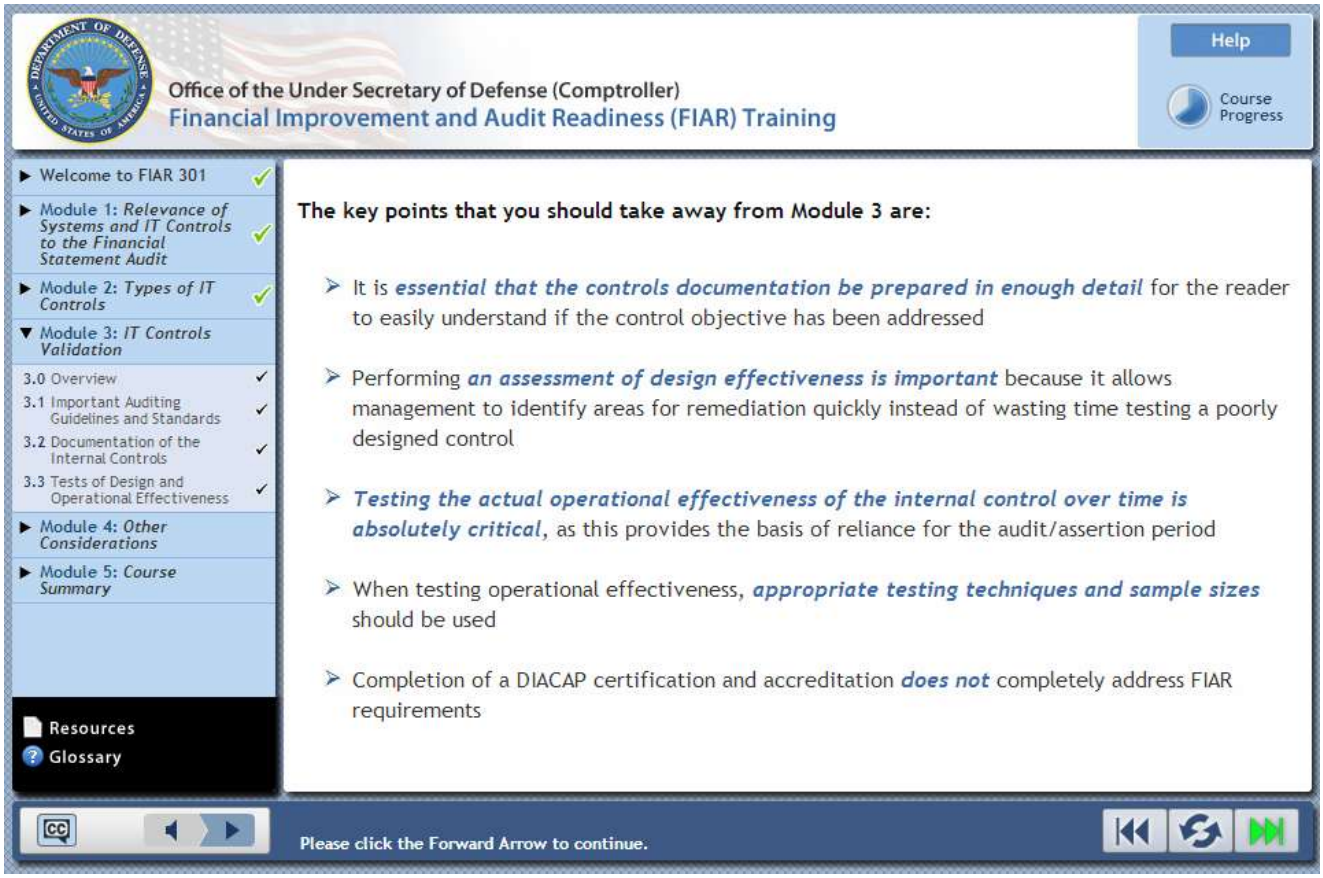
a) Incorrect. For controls performed annually, only one item is available for testing.
b) Incorrect. For controls performed quarterly, a minimum sample size of 2 is appropriate.
c) Incorrect. For controls performed monthly, a minimum sample size of 3 is appropriate.
d) Incorrect. For controls performed weekly, a minimum sample size of 10 is appropriate.
e) Correct! The appropriate sample size for a control performed once per day is 30.
f) Incorrect. For controls performed continuously, a minimum sample size of 45 is appropriate.



Module 3 Summary

An essential aspect for validating IT controls is the use of an appropriate methodology by the Reporting Entity when assessing its IT general and business process application controls. When evaluating IT application and general controls, the GAO FISCAM manual is the primary authoritative source for relevant control objectives and control techniques that should be included in the scope of the evaluation.

Please click the Forward arrow to continue.

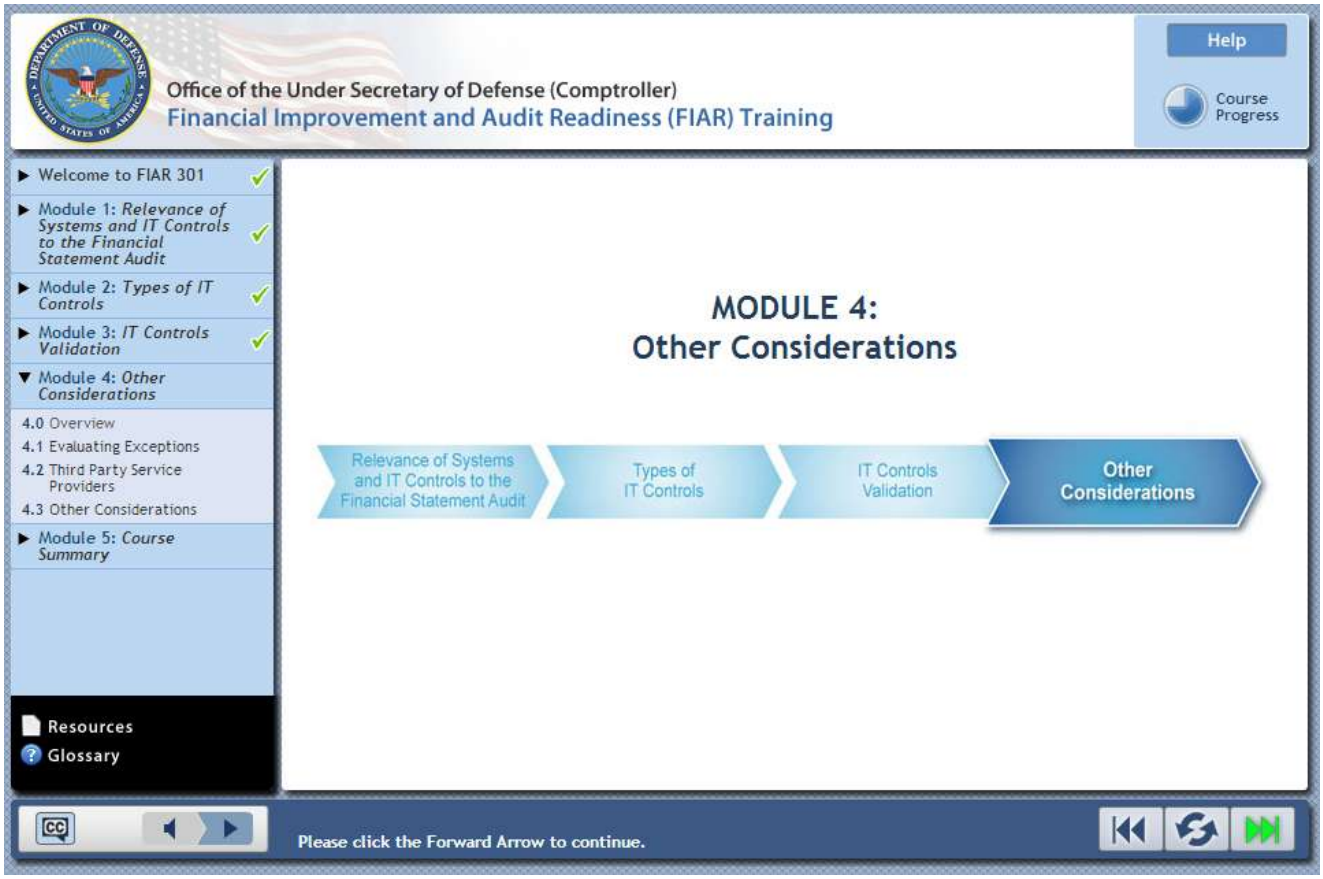


Module 3 Summary, continued

The key points that you should take away from this Module are that:

- It is essential that the controls documentation be prepared in enough detail for the reader to easily understand if the control objective has been addressed. Yes and No answers or the name of a policy are not sufficient.
- Performing an assessment of design effectiveness is important because it allows management to identify areas for remediation quickly instead of wasting time testing a poorly designed control.
- Testing the actual operational effectiveness of the internal control over time is absolutely critical, as this provides the basis of reliance for the audit/assertion period.
- When testing operational effectiveness, appropriate testing techniques and sample sizes should be used; and,
- Completion of a DIACAP certification and accreditation does not completely address FIAR requirements.

Please click the Forward arrow to continue.

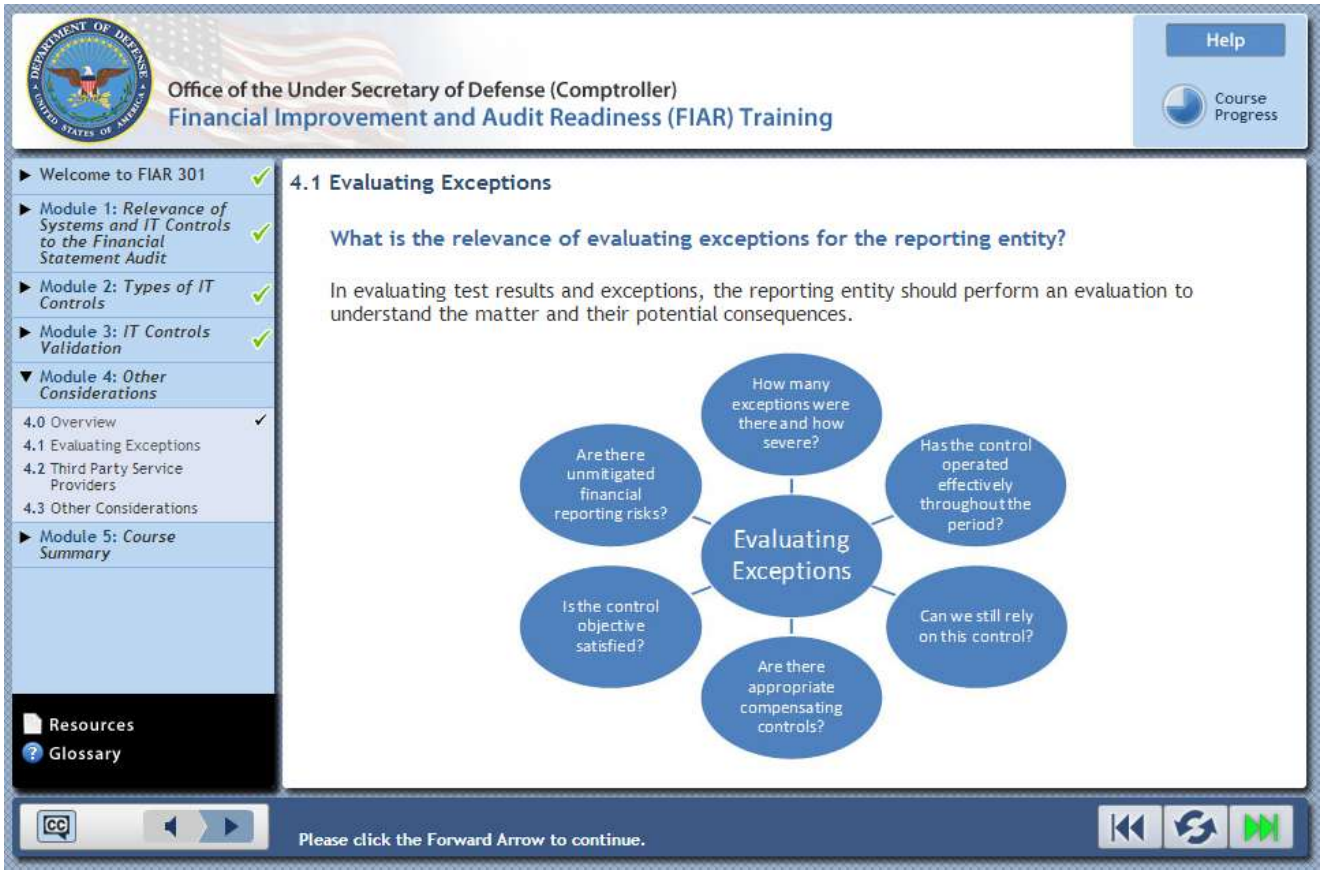


Module 4 Intro: Other Considerations

Now we will begin the fourth module.

This module introduces the other relevant IT controls audit readiness considerations, including exceptions encountered during testing, the role and impact of service organizations, and ability to recognize the different types of service auditor reports.

Please click the Forward arrow to continue.



4.1 Evaluating Exceptions

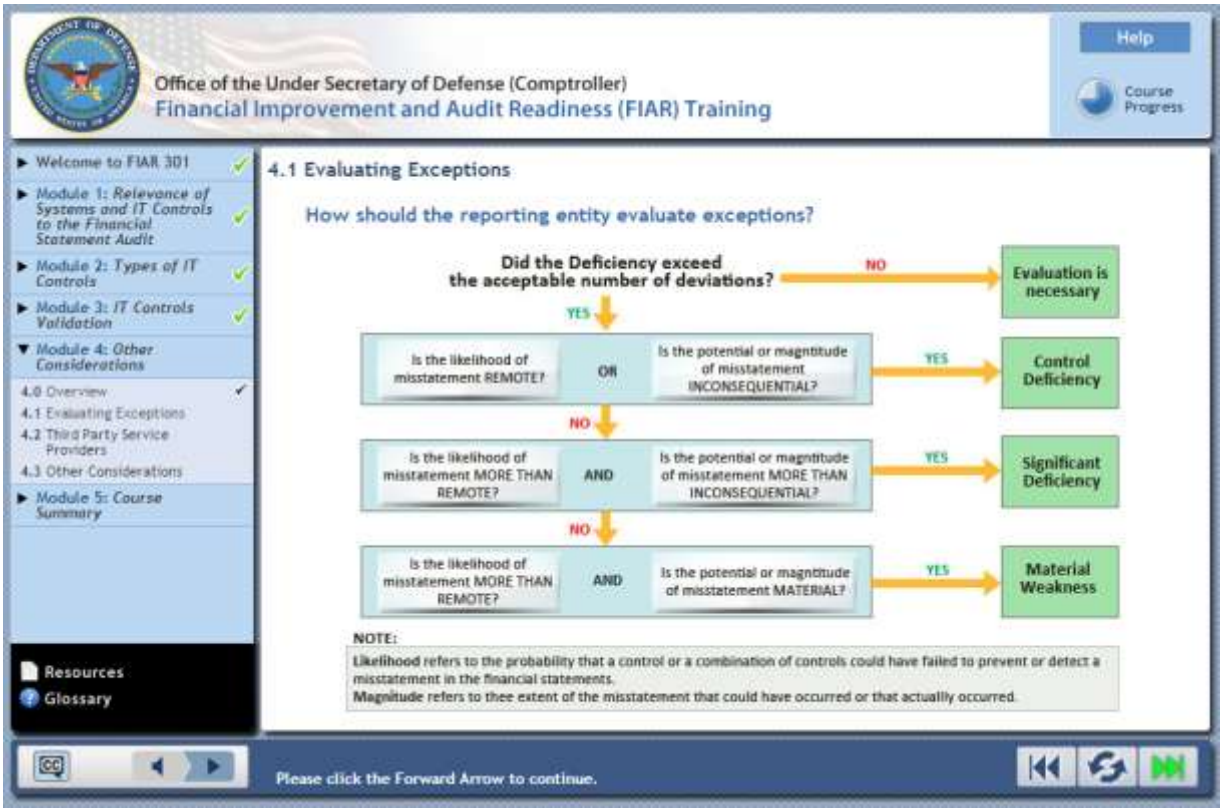
In evaluating test results and exceptions, the reporting entity should make evaluations to understand the matter and their potential consequences.

Test results will support management's judgment whether a control is functioning adequately or not. Exceptions noted in test-work over properly designed internal controls would indicate ineffectiveness. Management must consider the extent of a deficiency in such cases. Deficiencies can range from a control deficiency (such as missing initials indicating a supervisor's review on 1 of 26 reconciliations sampled); to a significant deficiency (such as only 8 monthly reconciliations were performed for the year); to a material weakness (such as reconciliation of several key accounts were not performed throughout the year, only at year-end). Points to consider include:

- How many exceptions were there and how severe?
- Has the control operated effectively throughout the period?
- Can we still rely on this control?
- Are there appropriate compensating controls?
- Is the control objective satisfied?
- Are there unmitigated financial reporting risks?

Internal control deficiencies are defined by the Public Company Accounting Oversight Board (or PCAOB) and the American Institute of Certified Public Accountants (or AICPA). GAO and OMB typically adopt these same definitions by reference into their own guidance.

Please click the Forward arrow to continue.



How should the reporting entity evaluate exceptions?

Let's discuss how the reporting entity can evaluate exceptions. A Control Deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements in a timely manner.

A deficiency in design exists when:

- A control necessary to meet the control objective is missing; or
- An existing control is not properly designed so that, even if the control operates as designed, the control objective would not be met.

A deficiency in operation exists when a properly designed control does not operate as designed; or the person performing the control does not possess the necessary authority or competency to perform the control effectively.

A Significant Deficiency is a control deficiency, or a combination of control deficiencies, that adversely affects the ability of DoD to initiate, authorize, record, process, or report external financial data reliably in accordance with Generally Accepted Accounting Principles such that there is a more-than-remote likelihood that the control will not operate to prevent or detect a more-than-inconsequential misstatement of the entity's financial statements.

A Material Weakness is a reportable condition, or combination of reportable conditions, that results in a more-than-remote likelihood that a material misstatement of the financial statements will not be prevented or detected.

For a more detailed review on the topic of evaluating exceptions for financial reporting, please refer to the FIAR Guidance Courses 101 and 102.

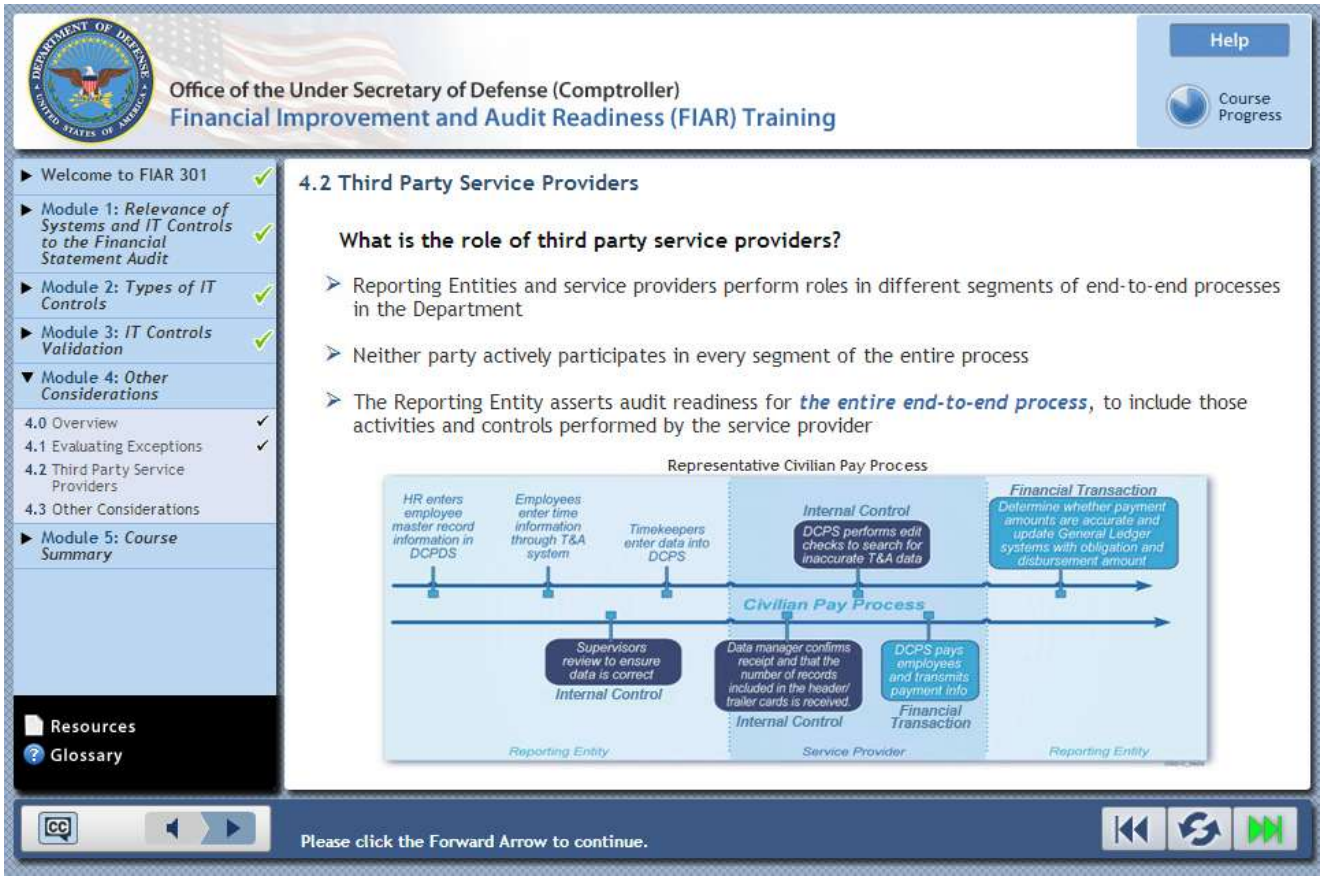
Please click the Forward arrow to continue.

A _____ is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis.

a) Deficiency
b) Significant Deficiency
c) Material Weakness
d) None of the above

Explanation

a) Incorrect. A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis.
b) Incorrect. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control, that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.
c) Correct! A material weakness a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis.
d) Incorrect. One of the answers listed is correct.



4.2 Third Party Service Providers

Reporting Entities and third party service providers perform important roles in different segments of end to-end business processes. Generally, neither party has complete control over a transaction from initiation through posting to the general ledger.

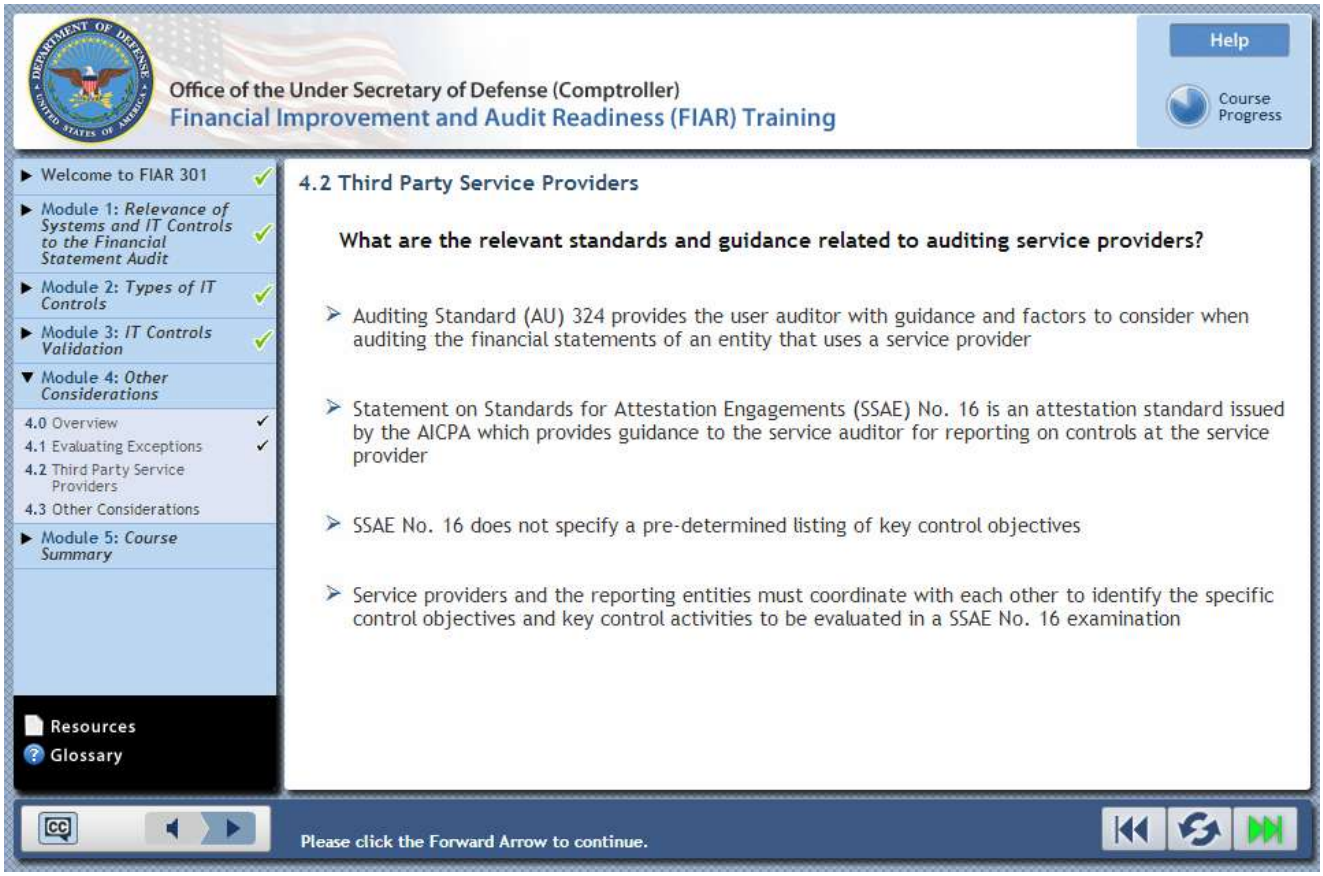
However, it is very important to note, that the Reporting Entity asserts audit readiness for the entire end to end process, to include those activities and controls performed by the service provider.

To illustrate this concept, we have provided a high level example of a representative Civilian Pay Process noting the roles of the Reporting Entity and service provider.

This example demonstrates the functional activities performed by the Reporting Entity and service provider from hiring a new employee and creating a new employee record in the personnel system, to entering time, through pay calculation, disbursing, and recording payroll expense in the general ledger.

Please note: Roles and responsibilities of third party service providers are discussed in-depth in FIAR 103.

Please click the Forward arrow to continue.



What are the relevant standards and guidance related to auditing service providers?

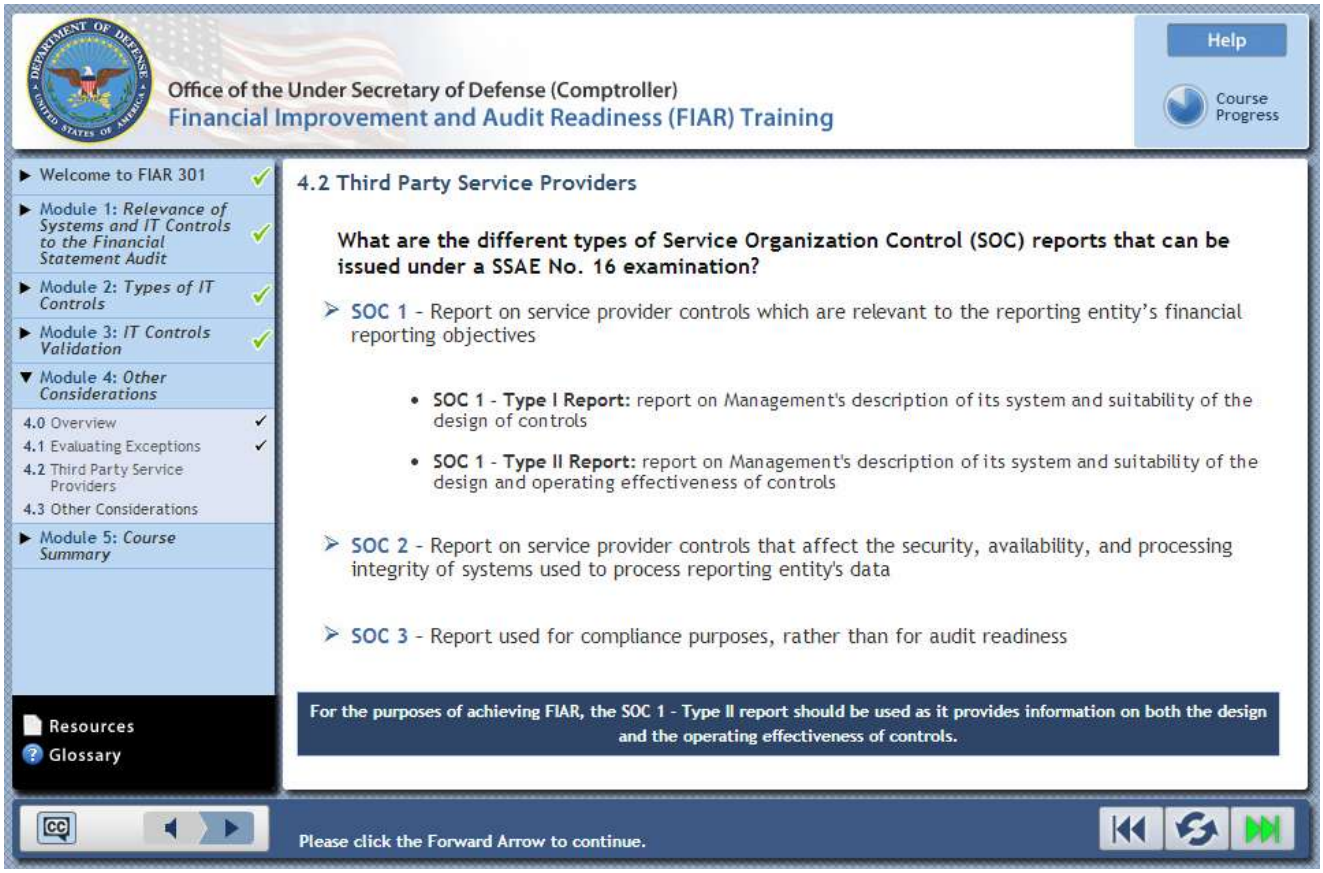
Let's discuss the relevant standards and guidance related to auditing service providers. There are two key standards that you should be familiar with:

Auditing Standard 324 (or AU 324) provides guidance on the factors the reporting entities independent auditor should consider when auditing the financial statements of an entity that uses a service provider.

Statement on Standards for Attestation Engagements No. 16 (or SSAE No. 16) is an attestation standard put forth by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA) that addresses engagements undertaken by a service auditor for reporting on controls at organizations (such as service organizations) that provide services to user entities (such as reporting entities), for which a service organization's controls are likely to be relevant to a user entities internal control over financial reporting (or ICOFR).

It is important to note that neither AU 324 or SSAE No. 16 specify a pre-determined set of control objectives or control activities that service providers must achieve. Therefore it is essential that the service providers and the reporting entities coordinate with each other to identify the specific control objectives and control activities to be evaluated in a SSAE No. 16 examination.

Please click forward arrow to continue.



What are the different types of Service Organization Control (SOC) reports that can be issued under a SSAE No. 16 examination?

Now that we have discussed the relevant standards for auditing service providers and reporting entities that use service providers, let's discuss the different reports that may be issued under a SSAE No. 16 examination.

In response to the evolving assurance needs of service organization customers, the AICPA has responded by designing multiple Service Organization Control (or SOC) reports. The reports are based on SSAE No. 16 and Trust Services (AT 101).

- Each SOC report has been purposefully developed to address a specific assurance need. For example, controls that affect user entities' financial reporting (SOC 1), or controls that affect the security, availability, and processing integrity of the systems or the confidentiality or privacy of the information processed for user entities' customers (SOC 2 and 3). The applicable SOC report will vary depending on the subject matter.

- The SOC 1 Report is the report that should be used for the purpose of FIAR requirements for Audit Readiness, as it is the report that states whether relevant key control objectives are met or not.

SOC 1 – Type I Report: The report on Management's Description of a Service Organization's System and the Suitability of Design of Controls. These reports encompass:

- The service auditor's report in which the service auditor expresses an opinion on the fairness of the presentation of management's description of the service provider's system; and, the suitability of the design of the controls to achieve the related control objectives included in the description as of a specified date;

- Management's description of the service organization's system; and

- Management's written assertion

SOC 1 – Type II Report: The report on Management's Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of Controls. These reports encompass:

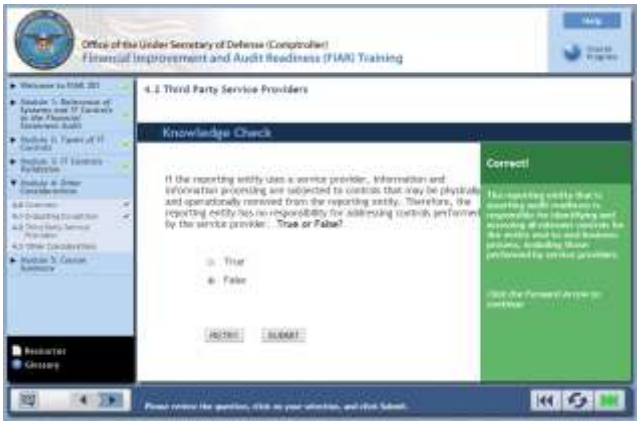
- The service auditor's report in which the service auditor expresses an opinion on the fairness of the presentation of management's description of the service provider's system; and, the suitability of the design and the operating effectiveness of the controls to achieve the related control objectives included in the description throughout a specified period;

- Management's description of the service provider's system; and

- Management's written assertion

A Type II report is more commonly used and provides an opinion on both the design and the operating effectiveness of controls. FIAR requires service providers to obtain Type II reports as these reports demonstrate both the design and the operating effectiveness of controls.

Please click Forward arrow to continue.

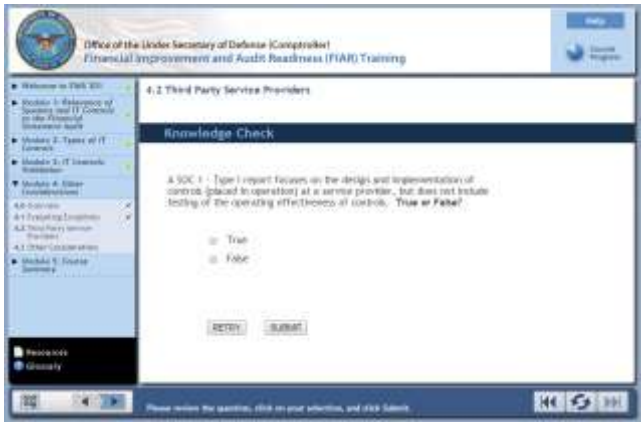


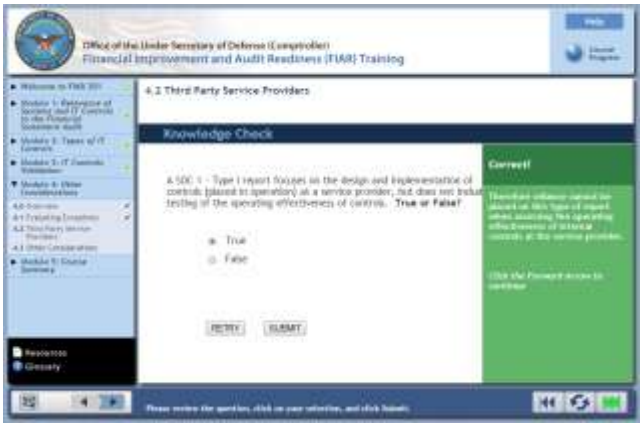
If the reporting entity uses a service provider, information and information processing are subjected to controls that may be physically and operationally removed from the reporting entity. Therefore, the reporting entity has no responsibility for addressing controls performed by the service provider. True or False?

Explanation

False: Correct! *The reporting entity that is asserting audit readiness is responsible for identifying and assessing all relevant controls for the entire end-to-end business process, including those performed by service providers.*

True: Incorrect. The reporting entity that is asserting audit readiness is responsible for identifying and assessing all relevant controls for the entire end-to-end business process, including those performed by service providers.

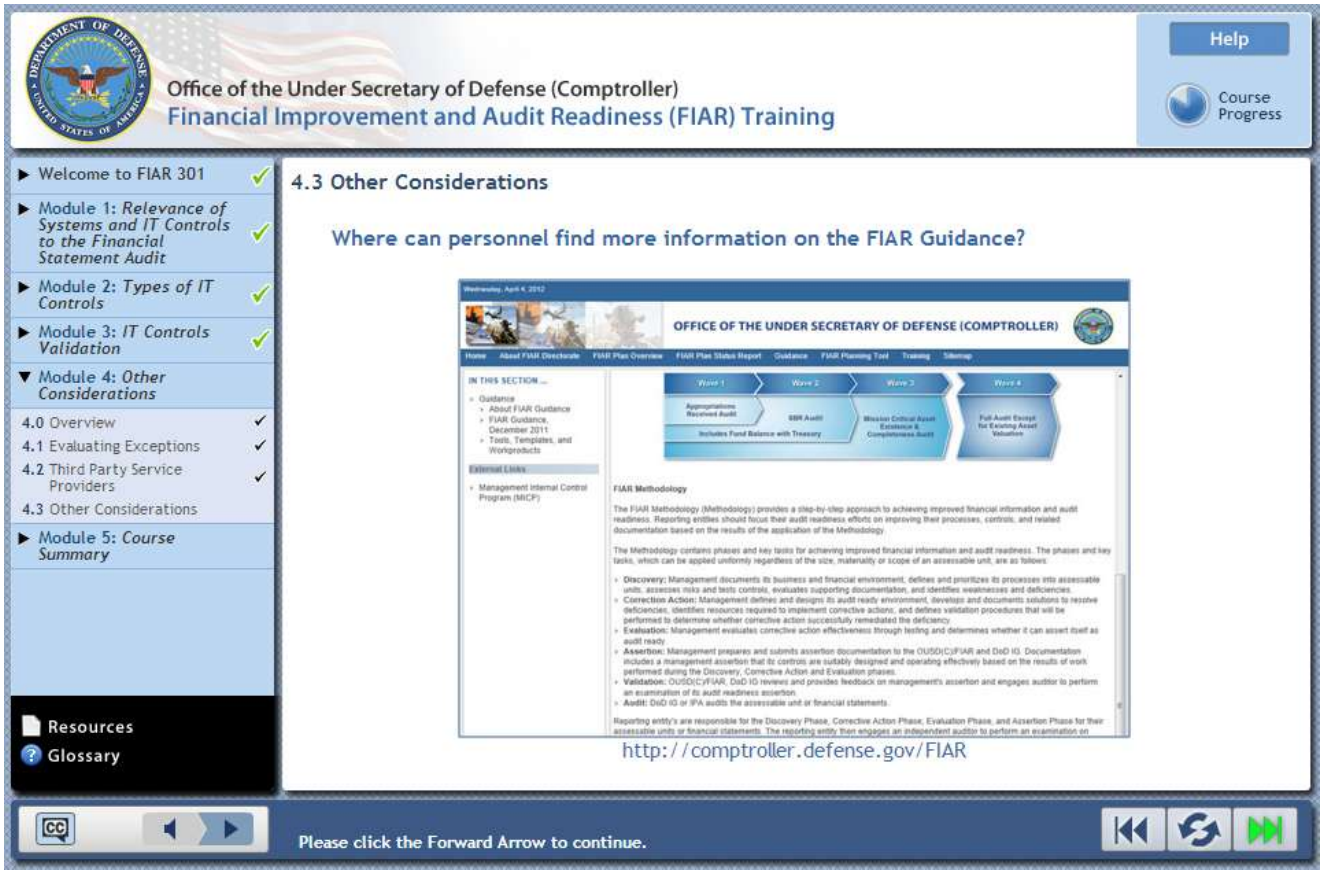




A SOC 1 - Type I report focuses on the design and implementation of controls (placed in operation) at a service provider, but does not include testing of the operating effectiveness of controls. True or False?

Explanation

> ***True: Correct!*** *Therefore reliance cannot be placed on this type of report when assessing the operating effectiveness of internal controls at the service provider.*
>
> *False: Incorrect. A SOC 1 - Type I report does focus on the design and implementation of controls (placed in operation) at a service provider and does not include testing of the operating effectiveness of controls.*



Where can personnel find more information on the FIAR Guidance?

Reporting entity personnel may access the FIAR Guidance on the OUSD(C) website. On the Comptroller's website, there is a link to the FIAR Guidance. The users are able to access a variety of documents through the Comptroller's website.

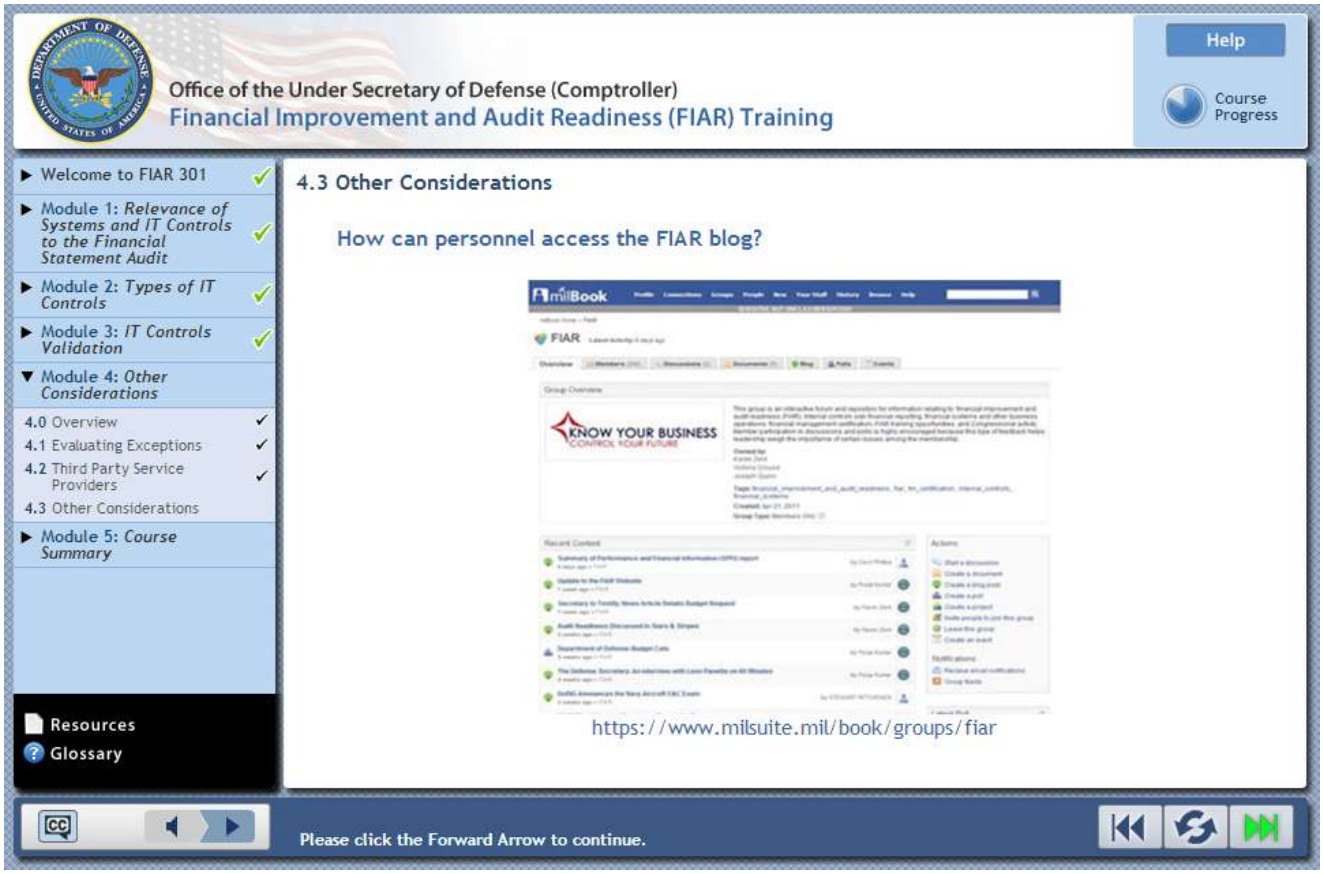
Users can access the FIAR Guidance, updated in December 2011, which details the FIAR Methodology we have discussed. The FIAR Guidance also details:

- FIAR Goal, Priorities and Strategy, including common challenges, integration of FIAR Methodology and OMB Circular A-123, Appendix A Requirements, Systems Transformation Initiatives, and Roles and Responsibilities; and,

- Appendices listing the material reporting entities (such as category 1, 2, and 3), key risks of material misstatements, key control objectives, and required key supporting documents.

In addition to the FIAR Guidance, the Comptroller's website also details various tools, templates, and example work products that can be used by reporting entities to achieve audit readiness.

Please click the Forward arrow to continue.

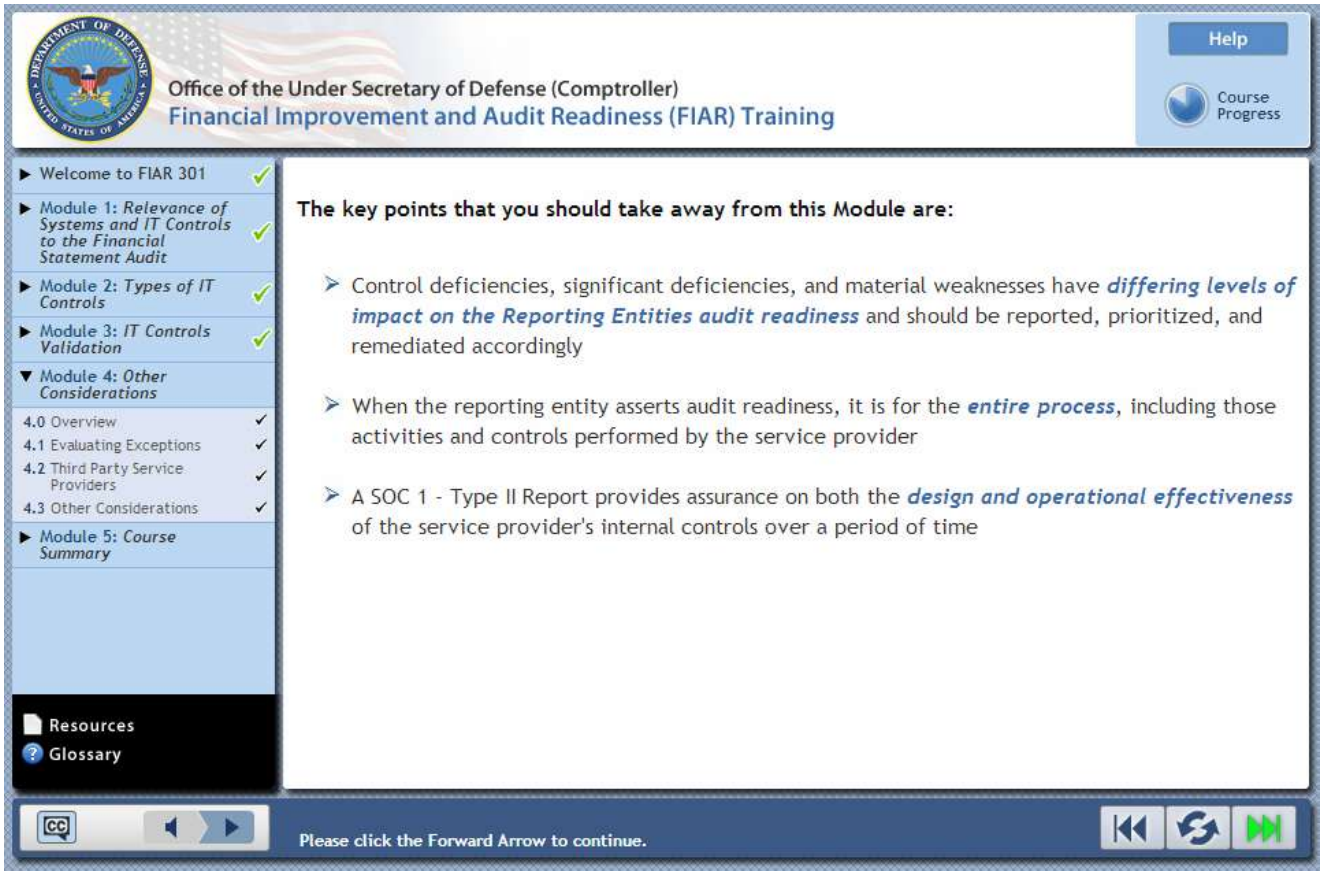


How can personnel access the FIAR blog?

You may be interested in visiting and joining the FIAR Blog. The FIAR Blog is becoming the primary way the FIAR Directorate communicates information. As other communications tools are created, such as Fact Sheets and Topics In Brief, they will be posted to the Documents section of the Blog for easy downloading and sharing.

To access the FIAR Blog, go to the link identified above - https://www.milsuite.mil/book/groups/fiar

Please click the Forward arrow to continue.

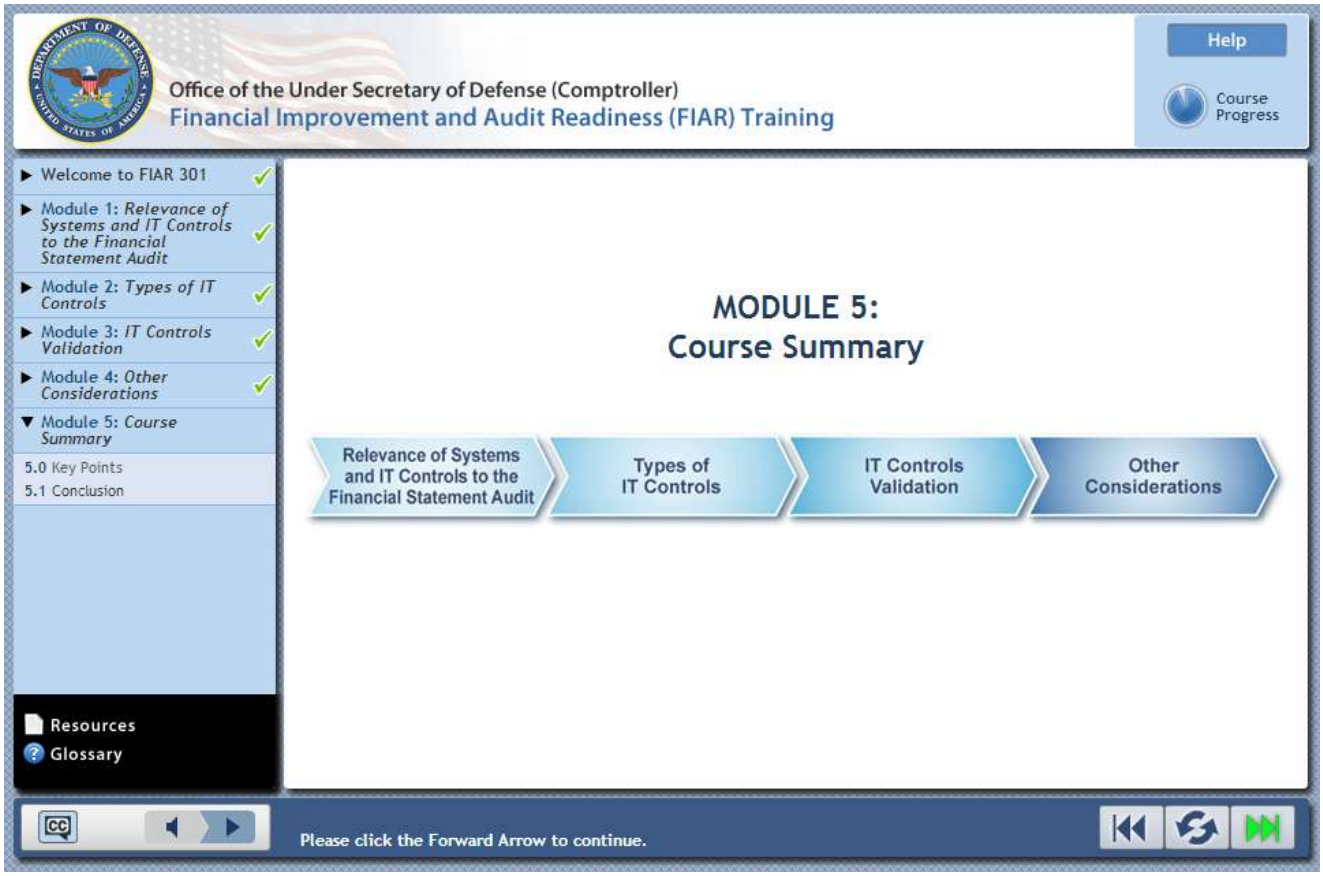


Module 4 Summary

The key points that you should take away from this Module are:

- Control deficiencies, significant deficiencies, and material weaknesses have differing levels of impact on the reporting entities audit readiness and should be reported, prioritized, and remediated accordingly;
- When the reporting entity asserts audit readiness, it is for the entire process including those activities and controls performed by the service provider; and
- A SOC 1 – Type II Report provides assurance on both the design and operational effectiveness of the service provider's internal controls over a period of time.

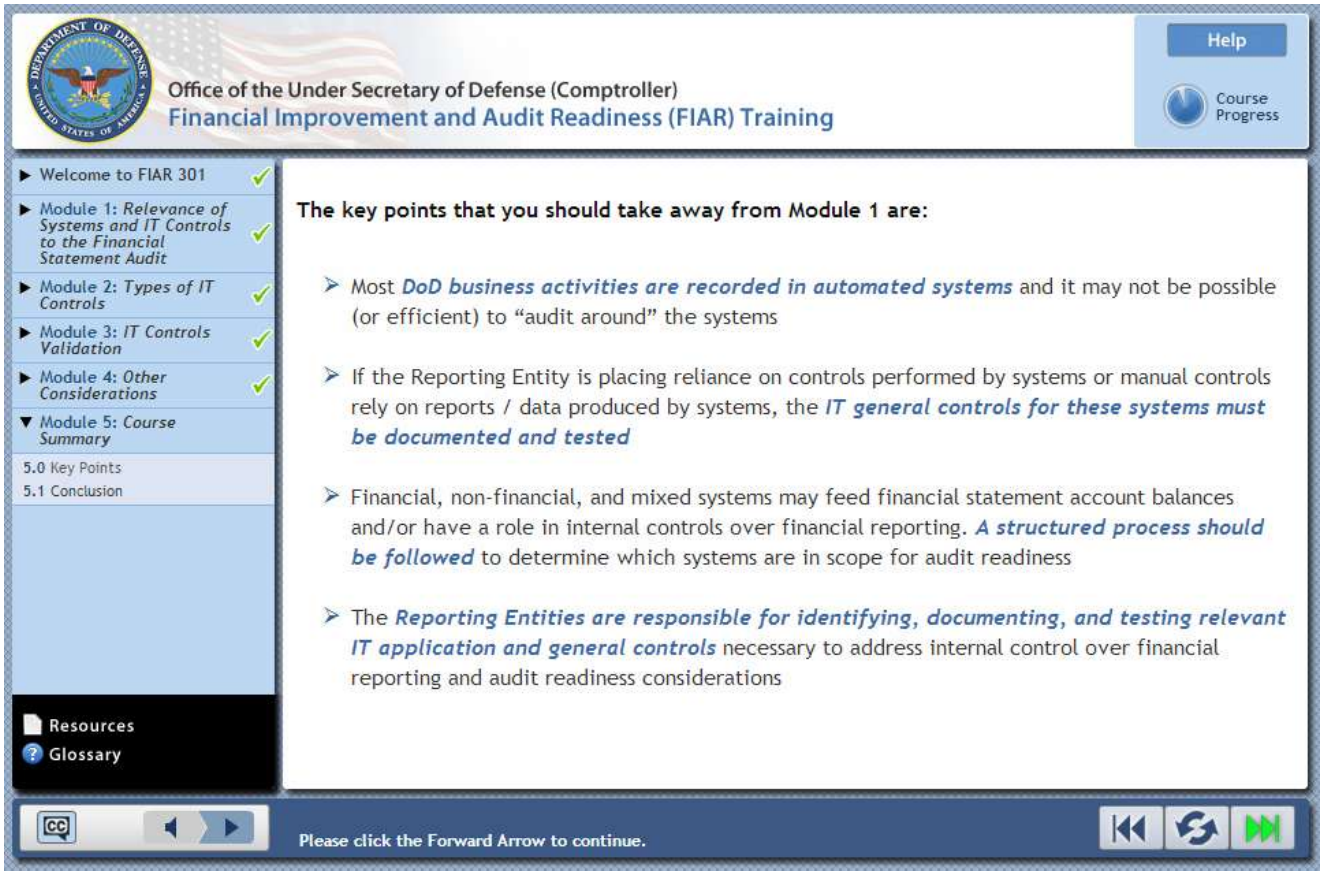
Please click the Forward arrow to continue.



Module 5 Intro: Course Summary

Now we will begin the fifth and final module. This module reviews the key points provided throughout this course regarding management's responsibilities for IT controls when preparing for a financial statement audit.

Please click the Forward arrow to continue.



Module 1 Summary

The key points that you should take away from Module 1 are that:

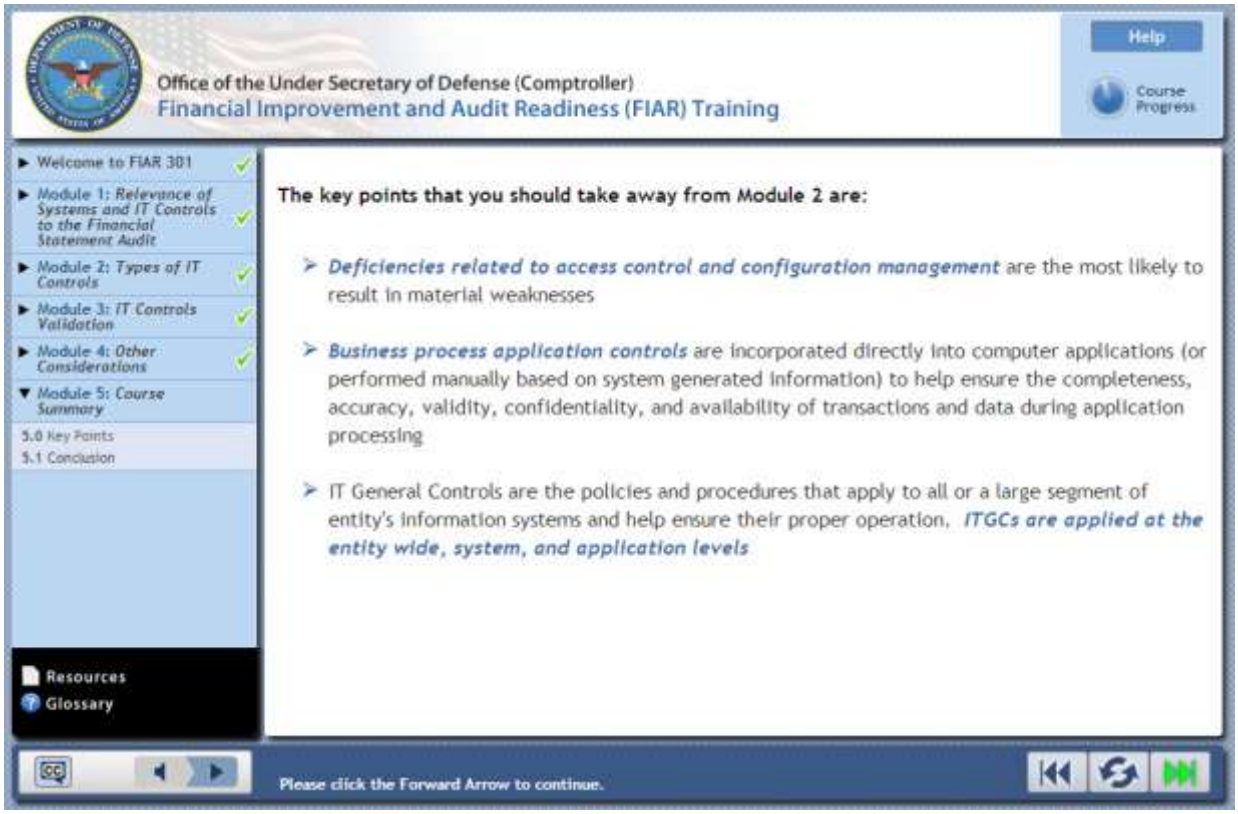
- Today, most DoD business transactions are recorded in computerized information systems and the DoD has a very complex and evolving systems environment. The flow of information from point of transaction initiation in source journals through posting in the general ledger and consolidation systems generally occurs electronically and supporting documentation may only exist in an electronic format. Given this dependence on computerized systems, it may not be possible to "audit around" these systems as physical source documentation may not exist. Even in those instances where it may be possible to "audit around" the Department's information systems, it will likely be inefficient to do so given the high volume of transactions and correspondingly large number of sample sizes required to audit around the system.

- It is essential to recognize that reliance on automated controls and manual controls that rely on system generated reports or data requires an understanding, documentation, and testing of IT general controls.

- Financial, non-financial, and mixed systems may impact financial statement account balances and/or have a role in internal controls over financial reporting. A structured process should be followed to determine which systems are in scope for audit readiness. This process should include the Statement to Process Analysis and Prioritize Key Tasks 1.1 and 1.2.

- The Reporting Entities are responsible for identifying, documenting, and testing relevant IT application and general controls necessary to address internal control over financial reporting and audit readiness considerations.

Please click the Forward arrow to continue.

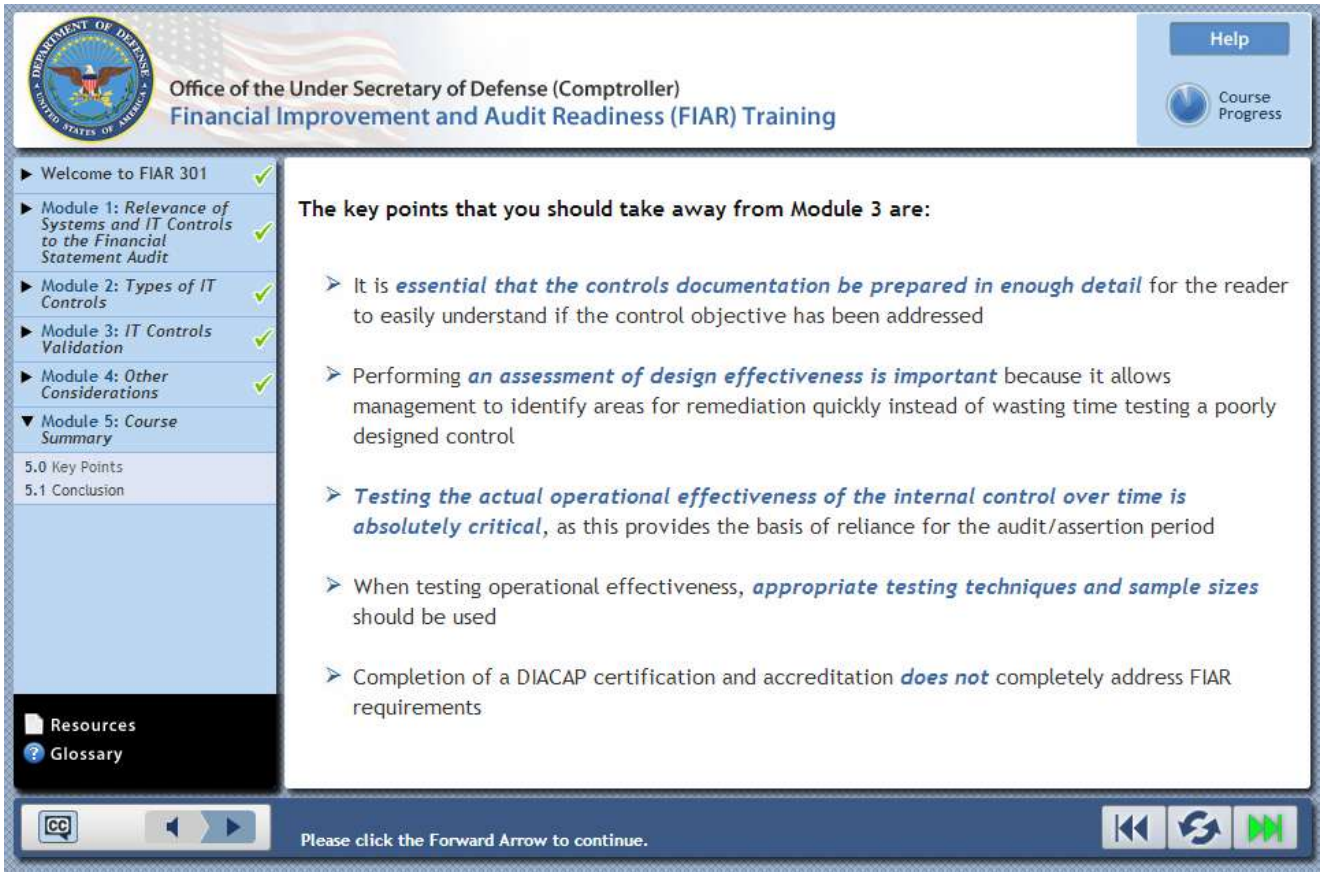


Module 2 Summary

The key points that you should take away from Module 2 are that:

- Deficiencies related to access control and configuration management are the most likely to result in material weaknesses.
- Business process application controls are incorporated directly into computer applications, or performed manually based on system generated information, to help ensure the completeness, accuracy, validity, confidentiality, and availability of transactions and data during application processing. Other application controls include:
  - Interface controls that are focused on the exchange of data between information systems and are primarily concerned with the completeness and accuracy of the data exchanged; and
  - Database Management System Controls that are focused on the integrity of the data that has been processed and stored by the information systems. A major area of emphasis is the ability to modify or delete processed data.
- IT General Controls (or ITGCs) are the policies and procedures that apply to all or a large segment of an entity's information systems and help ensure their proper operation. ITGCs are applied at the entity wide, system, and application levels. You may also recall that:
  - Entity wide ITGCs refer to controls in place across an entire organization;
  - System level ITGCs refer to controls in place across a common platform or computing environment; and
  - Application level ITGCs refer to controls that are unique to a specific application.

Please click the Forward arrow to continue.

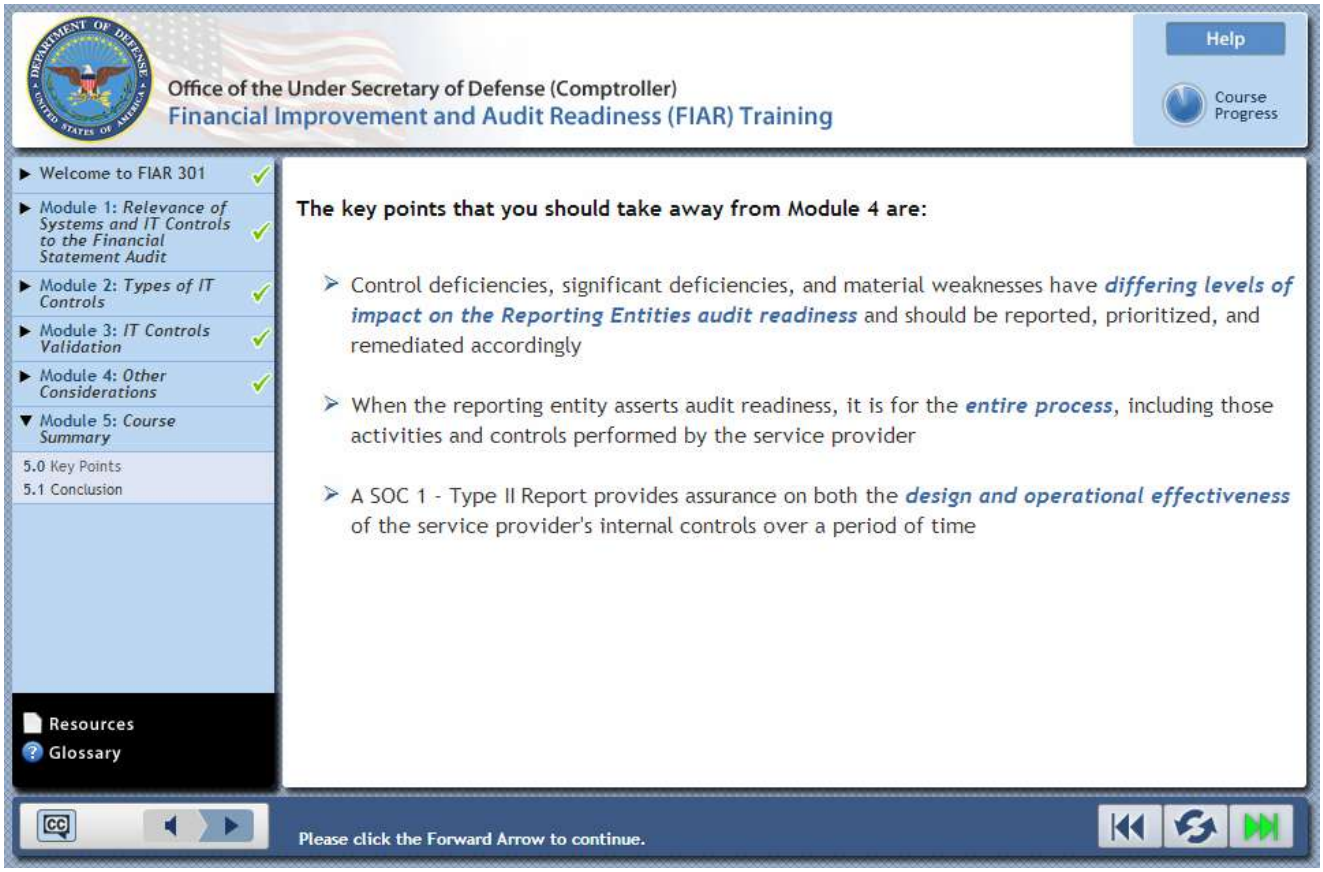


Module 3 Summary

The key points that you should take away from Module 3 are that:

- It is essential that the controls documentation be prepared in enough detail for the reader to easily understand if the control objective has been addressed -- Yes and No answers or the name of a policy are not sufficient;
- Performing an assessment of design effectiveness is important because it allows management to identify areas for remediation quickly instead of wasting time testing a poorly designed control;
- Testing the actual operational effectiveness of the internal control over time is absolutely critical, as this provides the basis of reliance for the audit/assertion period;
- When testing operational effectiveness, appropriate testing techniques and sample sizes should be used; and,
- Completion of a DIACAP certification and accreditation does not completely address FIAR requirements.

Please click the Forward arrow to continue.

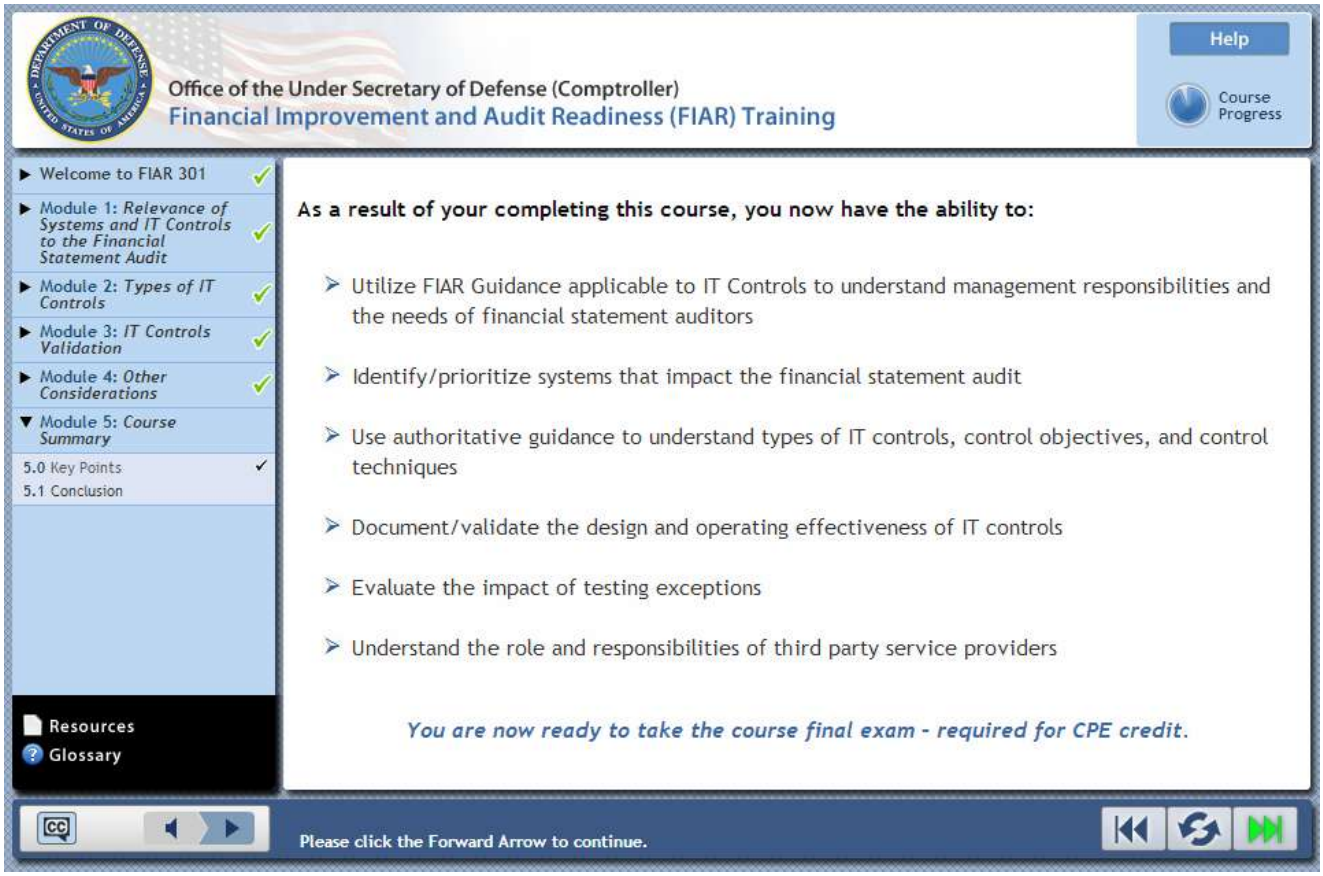


Module 4 Summary

The key points that you should take away from Module 4 are:

- Control deficiencies, significant deficiencies, and material weaknesses have differing levels of impact on the reporting entities audit readiness and should be reported, prioritized, and remediated accordingly;
- When the reporting entity asserts audit readiness, it is for the entire process including those activities and controls performed by the service provider; and
- A SOC 1 – Type II Report provides assurance on both the design and operational effectiveness of the service provider's internal controls over a period of time.

Please click the Forward arrow to continue.



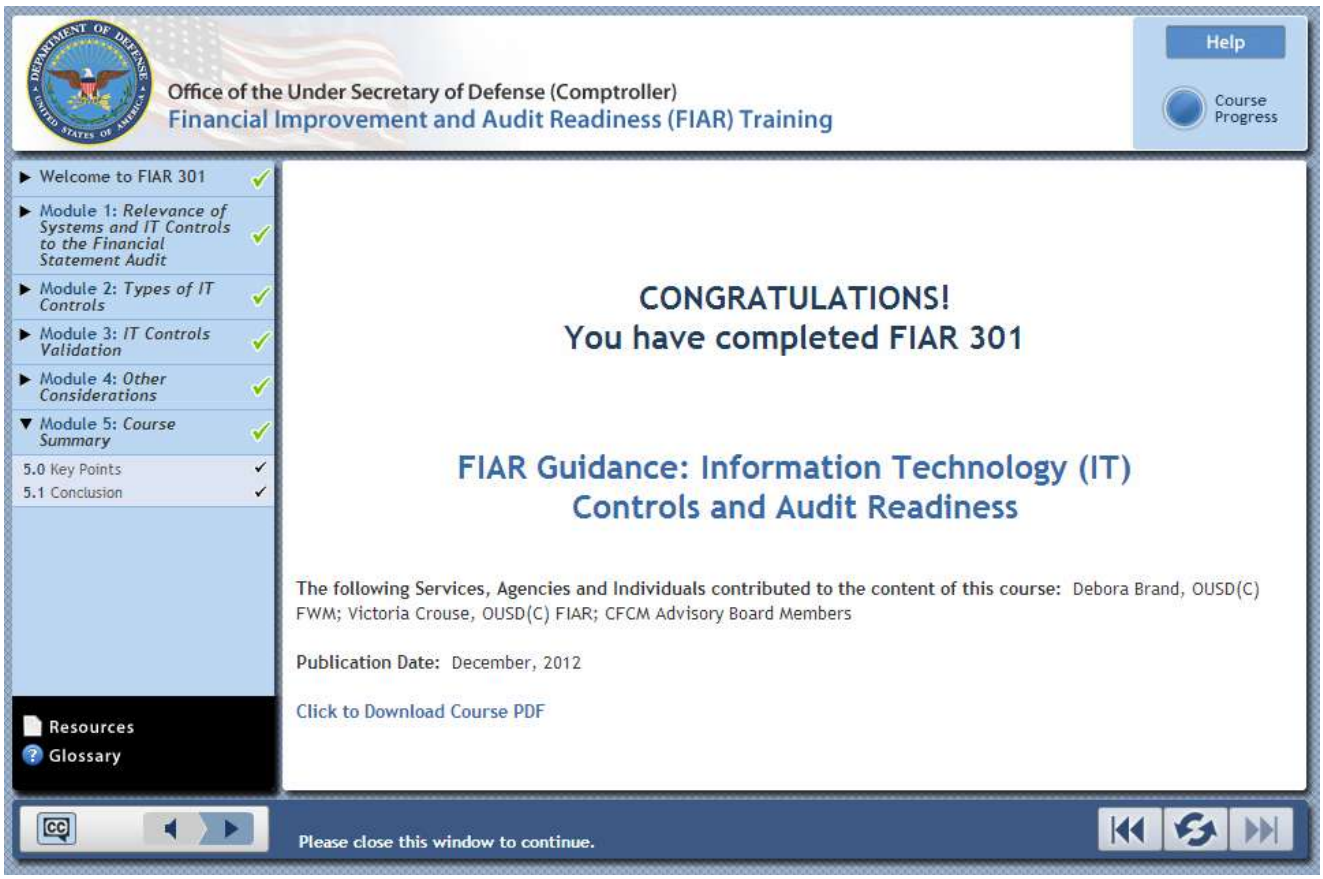
Course Summary

As a result of your completing this course, you now have the ability to:

- Utilize FIAR Guidance applicable to Information Technology Controls to understand management responsibilities and the needs of financial statement auditors;
- Identify and prioritize systems that impact the financial statement audit;
- Utilize authoritative guidance to understand the types of information technology controls, control objectives, and control techniques;
- Document and validate the design and operating effectiveness of information technology controls;
- Evaluate the impact of testing exceptions; and
- Understand the role and responsibilities of third party service providers.

You are now ready to take the final exam for this class which is required to obtain CPE credit.

Please click the Forward arrow to continue.



Conclusion

Congratulations on completing FIAR 301! You must complete the final exam for this class to obtain CPE credit.

Please close this window to continue.