This course supports the assessments for VLT2. The course covers 3 competencies and represents 3 competency units.

**Introduction**

**Overview**
The skills and knowledge measured by performance assessment VLT2 are derived from a survey of information security professionals from around the world and are also based on the many different information security and assurance frameworks (ISO 27001/2, COBIT, ITL, etc.). The results of this survey were used in weighing the subject areas and ensuring that the weighting is representative of the relative importance of the content.

The Security Policy and Standards subdomain focuses on creating organizational security activities and policies; assessing information security risk; and implementing and auditing information security management programs, information assurance certification programs, and security ethics.

Watch the following video for an introduction to this course:

**Competencies**
This course provides guidance to help you demonstrate the following 3 competencies:

- **Competency 427.3.2: Controls and Countermeasures**
  The graduate evaluates security threats and identifies and applies security controls based on analyses and industry standards and best practices.

- **Competency 427.3.3: Security Audits**
  The graduate evaluates the practice of defining and implementing a security audit and conducts an information security audit using industry best practices.

- **Competency 427.3.4: Certifications and Accreditations**
  The graduate identifies and discusses the Information Assurance certification and accreditation (C&A) process.

**Course Instructor Assistance**
As you prepare to successfully demonstrate competency in this subject, remember that course instructors stand ready to help you reach your educational goals. As subject matter experts, mentors enjoy and take pride in helping students become reflective learners, problem solvers, and critical thinkers. Course instructors are excited to hear from you and eager to work with you.

Successful students report that working with a course instructor is the key to their success. Course instructors are able to share tips on approaches, tools, and skills that can help you apply the content you're studying. They also provide guidance in assessment preparation strategies and troubleshoot areas of deficiency. Even if things don't work out on your first try, course instructors act as a support system to guide you through the revision process. You should expect to work with course instructors for the duration of your coursework, so you are
welcome to contact them as soon as you begin. Course instructors are fully committed to your success!

Preparing for Success

The information in this section is provided to detail the resources available for you to use as you complete this course.

Learning Resources
The learning resources listed in this section are required to complete the activities in this course. For many resources, WGU has provided automatic access through the course. However, you may need to manually enroll in or independently acquire other resources. Read the full instructions provided to ensure that you have access to all of your resources in a timely manner.

Automatically Enrolled Resources

You can access the learning resources listed in this section by clicking on the links provided throughout the course. You may be prompted to log in to the WGU student portal to access the resources.

SkillSoft and Books 24x7
You will access SkillSoft items at the activity level within this course. For more information on accessing SkillSoft items, please see the “Accessing SkillSoft Learning Resources” page.

The following textbook is available to you as an e-text within this course. You will be directly linked to the specific readings required within the activities that follow:


  *Note: Though this text is available in SkillSoft Books24x7, it is an invaluable reference for on-the-job situations, and you are encouraged to purchase your own copy.*


  *Note: These e-texts are available to you as part of your program tuition and fees, but you may purchase hard copies at your own expense through a retailer of your choice. If you choose to do so, please use the ISBN listed to ensure that you receive the correct edition.*

Pacing Guide
The pacing guide suggests a weekly structure to pace your completion of learning activities. It is
provided as a suggestion and does not represent a mandatory schedule. Follow the pacing guide carefully to complete the course in the suggested timeframe.


*Note: This pacing guide does not replace the course. Please continue to refer to the course for a comprehensive list of the resources and activities.*

### Controls and Countermeasures

In the world of information security, you often hear the terms *controls* and *countermeasures* used in the same sentence. Controls are the security measures put in place to prevent attacks or protect vulnerabilities. Countermeasures are the actions taken after vulnerability has been exploited or an attack has occurred. You learned quite a bit about different types of vulnerabilities, hacking, and countermeasures when working on the Ethical Hacking and the Vulnerabilities courses of study. Much of this material may seem familiar to you. You are revisiting this information because being an information security professional involves ensuring appropriate controls and countermeasures are identified as part of an information security management system.

### Security Controls and Best Practices

As you work your way through the activities, think about some of the security threats to the information assets at one of your current or former places of work. What vulnerabilities exist? What are some recommended best practices for security controls or countermeasures for these vulnerabilities?

This topic addresses the following competency:

- Competency 427.3.2: Controls and Countermeasures
  The graduate evaluates security threats, and identifies and applies security controls based on analyses and industry standards and best practices.

### Control and Methods of Attack

In this activity you will read five short chapters from *Information Security Management Handbook* in SkillSoft. Start with the following chapter:

- chapter 15 ("It Is All About Control")

This chapter explains controls in the context of measures that are put into operation to protect an organization from various threats.

The next set of chapters is in section 2.5 ("Methods of Attack"). This section outlines different types of threats that exist and recommends countermeasures.

Read the following four chapters:

- Chapter 72 ("Hacker Tools and Techniques")
As you read through the chapters, put together a matrix, such as this one, that compares the details of some of the threats that exist.

**Complete: RVLT Task 1 Performance Task**

Complete the following task in **TaskStream**:

- VLT2 Security Policies and Standards: RVLT Task 1

For details about this performance assessment, see the "Assessment" tab in this course.

**Threats vs. Vulnerabilities**

To learn about the differences between Threats and Vulnerabilities, click on **Threats and Vulnerabilities**.

**Designing an Information Security Management System (ISMS) for Your Organization**

In this section, you will apply what you learned in the Security Policy and Standards I Course of Study and begin the process of designing an information security management system (ISMS). Formally managing the information security function is a requirement in many organizations and should arguably be done formally in all organizations. A critical part of managing information security is the practice of preparing for and conducting an audit.

Audits force organizations to remain focused on practicing the ISMS controls and procedures throughout the everyday operation of the company. In order to implement an ISMS, organizations must define the scope and applicability of their information security requirements and document the controls that they will use to ensure suitable protection against threats and vulnerabilities. The audit is a process control that is used to ensure that the organization is doing the things that they committed to when developing and implementing the ISMS. Audits are not meant to be traps; instead, they are designed to be formal activities where practices are verified and new best practices are evaluated for inclusion in ensuing control and policy updates.

**ISMS Overview and Review (Policy and Standards)**

An information security management system (ISMS) represents a systematic approach to designing, implementing, maintaining, and auditing an organization's information system security objectives. As with any process, if an ISMS is not continually monitored, its effectiveness will deteriorate.

Most organizations perform important information security activities, but the majority of firms do not do so as part of an organization-wide initiative. When organizations place a strategic emphasis on a culture of securing their information assets, they increase the likelihood of
maintaining control of their information assets, and they lower their risk of losing customers, market share, or other resources due to a breach in confidentiality, integrity, and availability of key business assets.

As you read through the information in this section, pay particular attention to

- the differences in focus and application of the ISO 27001 and 27002 standards,
- the need for certification and standards organizations,
- the need and justification for establishing an ISMS, and
- the process and value of following a formal ISMS establishment methodology.

After reviewing this material and prior to beginning work on the performance tasks, keep the following things in mind in relation to the fabricated company you will learn about in your performance tasks:

- the organization's current security policy (if it has one)
- the organization's current ISMS (if it has one)
- the plan, do, check, act (PDCA) methodology
- the appendices recommended in each chapter
- the specific methodologies recommended
- the "as is" audit section and appendix tool

This topic addresses the following competencies:

- Competency 427.3.3: Security Audits
  The graduate evaluates the practice of defining and implementing a security audit and conducts an information security audit using industry best practices.

**Introduction to ISO Security Standards**

Review the following chapter in *How to Achieve 27001 Certification*:

- chapter 1 ("Introduction to International Standards Organization Security Standards")

This chapter introduces the International Standards Organization (ISO) security standards in general and focuses on the differences and relationship between ISO 27001 and ISO 27002. As you read through chapter 1, make sure that you are clear on the differences between the 27001 and 27002 standards. The differences are key points in determining which standard to use when defining and implementing an ISMS.

Review the following chapter in *How to Achieve 27001 Certification*:

- chapter 2 ("Information Security Management System")

This chapter introduces you to the concept of a formal ISMS, the foundation of the activities you will be completing to demonstrate your competency in this area. For many organizations, establishing a formal ISMS structure and discipline is the difference between success and
failure. Many organizations try to handle information security in an organic or IT specific way.

You will learn from reading this chapter that the companies that are purposeful and disciplined in their approach to information security are the ones that enjoy the greatest amount of control and utility over their information assets.

After you read through chapters 1 and 2, think about how you might apply the ISO standards in varying organizations. Do a little investigating to see if an organization you are affiliated with (place of employment, club, organization, etc.) has used the ISO standards in the past, and if so, to what end. If the organization has not previously used the ISO standards, find out why and if the organization might be interested in applying them now. If the organization is interested in applying the ISO standards, consider using this for your capstone project.

**ISMS: Concepts, Tools, and Implementation**

Review the following chapter in *How to Achieve 27001 Certification*:

- chapter 3 ("Foundational Concepts and Tools for an Information Security Management System")

This chapter expands on the security management framework (SMF) and introduces many concepts and tools to use during the establishment, implementation, operation, monitoring, review, maintenance, and improvement of information security and an information security management system.

Review the following chapter in *How to Achieve 27001 Certification*:

- chapter 4 ("Implementing an Information Security Management System-Plan-Do-Check-Act")

This chapter presents direction on how to implement an ISMS. The development of an ISMS is a systematic process, and the material in this chapter provides a description of the process, supporting tools, templates, and document outlines. In brief, the ISMS development process follows the plan-do-check-act (PDCA) model and uses security control detail from ISO 27002. The level of detail and documentation depends first on the security goals of the organization and second, on the desire to obtain ISO 27001 certification.

Review appendix C ("PDCA Guideline Documents-Outlines") in *How to Achieve 27001 Certification*.

This appendix is a template for setting up an ISMS implementation project. You should download the file and save it to your local drive so that you can modify it to fit your specific project.

Use the PDCA guidelines to do a walkthrough of your current organization or an organization you are affiliated with. What do you notice? What needs to be addressed? How would the PDCA help your organization enhance their security posture? Share your thoughts on the
message board.

**Complete: RVLT Tasks 2 and 3 Performance Tasks**

Complete the following task in TaskStream:

- VLT2 Security Policies and Standards: RVLT Task 2
- VLT2 Security Policies and Standards: RVLT Task 3

For details about this performance assessment, see the "Assessment" tab in this course.

**Ethics**

Organizations store, transact, and utilize tremendous amounts of sensitive data. System architects, administrators, and users all have ethical responsibilities for protecting privacy, anonymity, and other sensitive information assets. Before the conclusion of this course of study, you are going to learn about key ethical issues that must be part of an information security professional's professional code.

**Security Ethics**

As you complete the readings in this section and participate in the online discussions about security ethics, put yourself in each of these roles:

- the system administrator
- the system user
- the individual about whom information is being transacted
- the stakeholders of the organization

For each role, think about what your ethical responsibilities are, and also think about what your preferences and desires are related to how your sensitive information is being managed. Think about the costs of violating ethical cannons in both monetary and personal terms.

**Ethics Reading**

Read the following chapters in Information Security Management Handbook:

- chapter 56 ("Ethics and the Internet")
- chapter 57 ("Computer Ethics")

These chapters directly address the ethical issues that face IT and information security professionals. This content covers ethical cannons of information security in a networked, information-driven world.

*Note: This is not an assessed activity; however, you are strongly encouraged to participate. In order for this activity to be successful, you need complete the following two tasks.*

1. Post a response to the following prompt in the "Security Ethics" discussion thread on the message board.
Prompt: What are some key ethical issues that IT security professionals face? Mention any two that you would like to discuss and write a post in the discussion board detailing the ethical issues and your personal views of them. As you create your post, consider the following questions:

- Which ethical issue did you choose and why?
- How do you see organizations and IT professionals that you are familiar with addressing these issues?
- How would you revise the current practices in your own organization to suitably address these issues?

2. After making your own post, reply to the posts of two other students. Please remember to be appropriate and considerate in your replies. The following suggestions could guide you in responding to other students.

- Aspect: Do you agree or disagree that each of the ethical issues that were discussed are suitably addressed by the individual or organization? Why or why not?
  Feedback: Provide feedback to the student who wrote the initial post. Share why you agree or disagree with the issues that the student identified.
- Aspect: Do you have any experience with the issues that were discussed? If yes, explain how you handled them. If no, justify how you would address these issues.
  Feedback: Provide feedback to the student who wrote the initial post. Share why you agree or disagree with the best practices the student identified.

Note: It is recommended that you draft your posts in a word document prior to posting. This will help you create a clearly articulated, meaningful response.

Compliance Management

Review the following chapter in How to Achieve 27001 Certification:

- chapter 6 ("Compliance Management")

ISO 27001 is an important standard to map an ISMS to, but it is not the only one that an organization might encounter. Other compliance requirements are Sarbanes-Oxley, HIPAA, FISMA, and many other legislative and regulatory requirements. Certain industries also have their own compliance processes.

Chapter 6 presents an abstract approach to managing multiple standards, and introduces the security management framework (SMF), which can be applied as a single methodology for discovery, analysis, and reporting that establishes, tracks, and proves compliance with all applicable security requirements. You will be applying what you have learned in this chapter in the final performance task for this assessment.

Certification and Accreditation

Certification and accreditation is a process for establishing standards for certifying information
security systems. National security systems (i.e., government or federal information systems) must all be certified and accredited. Private industry does not need to follow the same guidelines; however, most enterprises do follow an internal certification and accreditation process based on different standards. In this section you will be introduced to different systems and frameworks related to information security systems and the varying processes surrounding them.

**Compliance With Standards**

In this topic you will learn about varying risk management frameworks and obtaining ISO 27001 certification. The governance frameworks you will learn about share many commonalities and serve many different purposes. Complete all the activities in this topic area-each activity is designed to help prepare you for the performance assessment.

This topic addresses the following competencies:

- Competency 427.3.4: Certifications and Accreditations
  The graduate identifies and discusses the information assurance certification and accreditation (C&A) process.

**Audit and Certification**

Review the following chapter in *How to Achieve 27001 Certification*:

- chapter 5 ("Audit and Certification")

When organizations go through the process of developing an ISMS using the International Standards Organization (ISO) standards, they benefit by managing risk in repeatable and purposeful ways.

Their overall business benefits from the structure and rigor that is required in order to properly manage and maintain an ISMS. Many companies choose to pursue independent auditing and certification that demonstrates that their ISMS meets the ISO standards. Chapter 5 presents the details for obtaining ISO 27001 certification.

Has the organization you currently work for achieved ISO certification? Chat with the information security professional in charge of the ISMS at an organization you are affiliated with about the process.

**Risk Management Framework**

The National Institute of Standards and Technology (NIST) provides standards for many different technologies and measurements. This non-regulatory federal agency is housed within the U.S. Department of Commerce. As an information security professional you will use many of the NIST’s standards.

Create a ready reference for yourself using *Guide for Applying Risk Management Framework to Federal Information Systems*, which outlines the six-step process for using a risk management framework. Include all the information necessary to fill out this table completely:

<table>
<thead>
<tr>
<th>Rmf Step 1 — Categorize Information System</th>
<th>Individual tasks to complete for this step</th>
<th>Where to go for additional guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rmf Step 2 — Select Security Controls</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rmf Step 3 — Implement Security Controls</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rmf Step 4 — Assess Security Controls</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rmf Step 5 — Authorize Information System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rmf Step 6 — Monitor Security Controls</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Governance Frameworks**

There are several governance frameworks that exist to help IT set priorities and match them to the goals of business. In this activity you will learn about four different frameworks: COBIT, ITIL, NIST, and ISO. Each framework lends itself to a particular aspect of enterprise security. Organizations often use a combination of frameworks to ensure the control strategies they employ are effective.

Read the following:

- *COBIT Mapping: Mapping of ITIL V3 With COBIT 4.1*,
- *COBIT Mapping: Mapping of NIST SP800-53 Rev 1 With COBIT 4.1*, and

Create a matrix similar to the one below. This will help you to gain a better understanding of the different frameworks and when and where each may be used.

<table>
<thead>
<tr>
<th>Framework</th>
<th>Industry framework used most frequently</th>
<th>Purpose of framework design/organization</th>
<th>Strengths of framework</th>
<th>Weaknesses of framework</th>
<th>Is there a certification/accreditation processes?</th>
<th>When would you use this framework?</th>
</tr>
</thead>
<tbody>
<tr>
<td>COBIT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
C&A Process

For this activity, you are going to go on a quest for information related to the certification and accreditation (C&A) processes that exist. On your quest you will run into information about FISMA, NIST, DITSCAP, and NIACAP. FISMA is the law that mandates all federal information systems be certified and accredited. NIST, DITSCAP, and NIACAP are methodologies used by federal agencies for the C&A process. Using a search engine, search for each of the terms above to obtain more information about the process.

Non-federal information systems are not required to be certified and accredited like federal agencies. Most organizations follow their own C&A process.

"A Certification and Accreditation Plan for Information Systems Security Programs," published by the Sans Institute, is an excellent resource.

Create an informational matrix, similar to the one below, that outlines the C&A process for both federal and non-federal information systems. You will need this information for one of your performance assessments.

<table>
<thead>
<tr>
<th>Types of Information System</th>
<th>Laws Guiding C&amp;A</th>
<th>Methodologies Used for C&amp;A</th>
<th>Specific Details/Comments About the Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federal</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Non-Federal</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Complete: RVLT Task 4 Performance Task

Complete the following task in TaskStream:

- VLT2 Security Policies and Standards: RVLT Task 4

For details about this performance assessment, see the "Assessment" tab in this course.

Final Steps

Congratulations on completing the activities in this course! This course has prepared you to complete the assessments associated with this course. If you have not already been directed to complete the assessments, schedule and complete your assessments now.