# International Certificate in Security Management
# Unit 1:  Introduction to Security Management

## Instructions to candidates:

1. **Complete all details requested below.**
2. **Please read through all the questions and then write your answers.**
3. **Once you have completed this assessment document, please save as a single Microsoft Word document, and submit all pages using the correct submission upload link.**

**Should you have any difficulties, please email office@ebssa.net or call us on +39 3421872010**

| | | |
|---|---|---|
| Student Name | | MIHAELA NITA |
| Student ID:<br>#1243-0823 | | 437 MIHA |
| Is this a re-submission?<br>*If yes please submit by email to office@ebssa.net.* | | NO |
| Word Count:<br>*(This isthe number of words that you have written in each task, and does not include your assignment title, diagrams/appendices or bibliography)* | Task 1: | 764 |
| | Task 2: | 823 |
| | Task 3: | 770 |

When you have completed the 3 tasks shown on the following pages, please make sure you read through your answers and ensure that you have answered all the questions, addressed all the required learning outcomes and that the Plagiarism Statement below is signed and dated.

## Plagiarism Statement

I confirm that the work submitted is my own and no plagarism has been committed.

Signed: MIHAELA NITA

Dated: 03/03/2024

# Module 1

# Introduction to Security Management Assignment

## Scenario:

You have been approached by one of your company's directors who wishes to know more about security management. You may assume that she has limited knowledge of security and that any technical terms need to be explained.

The **3** tasks to be completed are shown on the following pages with the required learning outcomes. You need to answer the questions in each task, ensuring that within your answer you have covered the learning outcomes. All learning outcomes must be addressed to pass this assignment.

**Please answer all parts of the question using your own words. Copying and pasting text from the compendium could be classed as plagiarism.**

When you have completed the 3 tasks shown on the following pages, please make sure you read through your answers and ensure that you have addressed all the required learning outcomes and the Plagiarism Statement on the previous page has been signed.

You can then submit your assignment directly to the online course platform ensuring you upload the complete document against the correct submission link.

# Assignment Unit 1: Introduction to Security Management

**Please answer all questions within each task, taking in to account the guideline word count.**

| | | |
|---|---|---|
| **Task 1** | Explain what risk management means and illustrate how risk should be determined by calculating likelihood of risk and potential impact.<br>Explain the three stages of risk management AND identify three strategies for managing risk.<br>Explain what contingency planning means and why it is important. | **Guideline word count for Task 1**<br>**750** |

*Task 1 will be assessed based on the following criteria. Please ensure you answer all parts of the task, using your own words and ensuring that within your answers the following assessment criteria are addressed. To assist with this, read through your answer and tick the assessment criteria as you confirm they have been addressed.*

| **Outcomes of learning** | | **Assessment criteria** | | **Included in answer** |
|---|---|---|---|---|
| 1 | Understand organisational risk management | 1.1. | Explain the three stages of risk management | RiskAssessment<br>Risk Control<br>Contingency Planning |
| | | 1.2. | Analyse the relationship between risk, likelihood, and impact | |
| | | 1.3. | Explain the different types of risk management strategy organisations use | |
| | | 1.4. | Explain what is meant by contingency planning | |

Security has become increasingly important in all aspects of life in the 21st century, affecting how we live, travel, communicate, and manage risk. The role of the Security Manager has expanded to include dealing with terrorism, cybersecurity, risk and crisis management, business operations, and personal protection. Security Managers must operate in a tight financial environment and justify their systems, personnel, and budget to the Board of Directors.

The modern Security Manager is expected to have professional development and technical excellence, with more academically qualified and mixed-gender professionals in the field. Security management aims to create a safe environment for routine activities while considering the perceived level of threat. Risk management in security management involves balancing freedom and security, considering factors like operating environment, risk culture, resources, and strategic objectives. Strategies include avoiding risks, reducing risks through protocols, sharing risks to minimize liabilities, transferring risks through insurance or outsourcing, and retaining risks when acceptable or unmanageable.

Modern security management goes beyond traditional protection and requires a comprehensive approach to address present-day challenges. Security managers need a strong understanding of underlying principles for effective security management. Security management aims to strike a balance between freedom and security while considering numerous factors and employing appropriate risk management strategies.

The three basic concepts of security management are security, freedom of action, and the threat. Security and freedom are inversely linked, requiring a careful balance to determine the appropriate level of security. Understanding the level of threat is crucial for assessing the appropriate security measures, as exemplified by airport security checks. Risk management involves identifying potential risks, assessing their likelihood and impact, and implementing controls to minimize their occurrence and impact. The first stage, risk assessment, involves identifying potential threats and categorizing them based on likelihood and impact using a risk matrix. The second stage, risk control, involves implementing security protocols and procedures to minimize the likelihood and impact of identified risks. The third stage, contingency planning, involves developing plans to respond to and recover from security incidents. Effective risk management is essential for security managers to ensure the safety and security of their organizations. Total Security Management (TSM) aims to create safety proactively rather than reacting to risks and threats.

The Gold, Silver, Bronze (GSB) command system is used worldwide to manage multi-team operations. It involves creating a Command and Control (C&C) structure for effective daily operations. The three-tiered management structure consists of Gold (Strategic Management), Silver (Tactical Management), and Bronze (Operational Management) levels. Bronze Command conducts operational tasks, Silver Command ensures effective work, and Gold Command creates the overall strategy. The GSB system allows different commanders to coordinate actions with similar-level commanders in different systems for effective multi-team working.

Security in Depth is a cybersecurity strategy that involves multiple layers of defence to protect data and systems. It includes controls such as network segmentation, access control, and encryption. Involving everyone in security awareness enhances the ability to identify and address potential problems before they escalate.

Security managers must strike a balance between freedom and security, considering the actual level of threat and the impact on organizational activities. As we know, we will never run out of threats, and the likelihood is that however many threats we think of, the world will throw a new one at you that we had not taken into consideration.

Effective security management capability requires embedding programs and protocols into the organization's culture and operating procedures. Security managers can self-audit their organizations to identify vulnerabilities and potential issues. Overly intrusive control systems can lead to non-compliance and a culture of ignoring guidelines. Early detection of potential problems allows for smoother and more effective handling. Organizational complexity can increase the likelihood of problems and breakdowns in information transfer.

The Contingency Planning model is based on the idea that the person can identify all threats and the protocols can prevent them and in this way is create a safe company. The most important is detect and prevention all threats. When some incidence occurred because a wrong decision was made of someone from the company (forget the key on the gate) have a negative impact from the normal development of the operation. The response with the action which can have a fast solution, is needed to use a mixt of procedures and pre -planned options and find the right and fast way, have the ability to manage the situation and transmit to the team, work effectively under pressure. Use the training and also de resilience, deal with the consequence and find the best way to respond is the most important skill in the contingency planning.

One of the prevalent approaches to security management is the 'Threat-Based Management' model, has emerged as a prevalent approach to security management. as outlined in the three-step Risk Assessment - Risk Control - Contingency Planning.

This model operates on the premise that by identifying all potential threats and establishing protocols to mitigate them, an organization can ensure its safety. However, the challenge lies in the fact that the number of threats is endless, and no matter how many are anticipated or are considered, there is always the possibility of encountering unforeseen threats., the world tends to present unforeseen threats that were not initially anticipated.

The primary objective of TSM security is to optimize and minimize specific aspects of a company's operations. It strives to minimize risks and expenses, including theft, while enhancing areas such as procedural fairness and asset management. Ultimately, it endeavours to enhance the reputation and positive perception of the company's brand. Total security management aims to enhance security measures and minimize expenses through various strategies. Initially, a thorough examination of the entire supply chain is conducted, comparing the source of goods, the transportation route, and the method of transportation in terms of both cost-effectiveness and security. The optimal approach combines affordability with elevated levels of security, striving to strike a balance between the two aspects. Furthermore, the organization implementing comprehensive supply chain management will conduct thorough evaluations of the contractors it engages in foreign nations. By conducting staff screenings, the company aims to mitigate security risks such as theft, fraud, and terrorism. Additionally, the company diligently researches all applicable laws and tariffs along the supply route. Exploring alternative routes may provide enhanced safety measures or potentially lower tariffs. Defence in depth is a comprehensive approach that utilizes various security measures to safeguard an organization's valuable assets.

The underlying concept is to have multiple layers of defence in place, so that if one layer is breached, there are additional layers to prevent any threats from progressing further. This strategy not only tackles the security vulnerabilities associated with hardware and software, but also takes into account the potential risks posed by human factors such as negligence or human error, which are frequently responsible for security breaches.

The scale and complexity of cyber threats are increasing at an alarming rate. To safeguard an organization's endpoints, data, applications, and networks, a comprehensive defence in depth strategy is crucial. This approach utilizes advanced security tools to not only prevent cyber threats from occurring but also to effectively counter ongoing attacks, minimizing further damage.

Gold, Silver, Bronze Command the Three-Tiered Security Management System. Bronze Command level is the lowest tier within the command hierarchy, consisting of individuals and teams tasked with carrying out operational duties. Known as the Operational Command, this level may require interaction with the public, such as security teams in hotels, airports, or other public locations. Bronze teams primarily operate on the field and are usually the first responders who remain updated on current situations. In addition to fulfilling their designated responsibilities, they also play a crucial role in providing accurate and timely information to Silver and Gold Commanders, ensuring smooth communication up the chain of command. Silver Command is the commander which is responsible for creating work protocols and make al work, Gold Command is responsible for creating the full strategy. Executive Leadership: Entrusted with the overarching accountability for information security, which encompasses key organizational positions like the CSO and others. These top-tier roles typically supervise the development and implementation of the enterprise's information security strategy to safeguard information assets.

Information System Security Professionals are accountable for the creation, execution, supervision, and assessment of security protocols, norms, benchmarks, procedures, and guidelines within an organization. Examples of such roles encompass but are not restricted to IT security manager, IT risk management manager, compliance manager, IT security analyst, and more.

Data Custodians are responsible for overseeing the system/databases, even if they do not own them, for a certain duration. Typically, this role falls under network administration or operations, which are the individuals who typically manage the systems on behalf of the owners. Data Owners, on the other hand, are the individuals who have ownership of the data, information, or systems and have the authority over the budget. Their responsibilities include ensuring that the security measures align with the organization's security policy, establishing the sensitivity or classification levels, and determining access privileges.

Users are held accountable for the utilization of resources and the protection of availability, integrity, and confidentiality of assets. They have an obligation to comply with the security policy to safeguard the organization's interests. On the other hand, IS Auditors have distinct responsibilities. They provide unbiased assurance to management regarding the suitability of the security objectives in place. Furthermore, they assess the adequacy and effectiveness of the security policy, standards, baselines, procedures, and guidelines in meeting the organization's security objectives. Additionally, they identify whether the established objectives and controls are being successfully accomplished.

<table>
<tr><td colspan="5"></td></tr>
<tr><td colspan="2"><b>Task 3</b></td><td colspan="2">Explain the preparedness cycle and why it is important.<br>Giving three examples of different departments, explain how security management supports other departments within a company.<br>State the importance of regular reviews of security plans and procedures, what factors may change security plans and procedures and what may happen if these reviews are not carried out.</td><td><b>Guideline word count for Task 3</b><br><b>750</b></td></tr>
<tr><td colspan="5"><i>Task 3 will be assessed based on the following criteria. Please ensure you answer all parts of the task, using your own words and ensuring that within your answers the following assessment criteria are addressed. To assist with this, read through your answer and tick the assessment criteria as you confirm they have been addressed.</i></td></tr>
<tr><td colspan="2"><b>Outcomes of learning</b></td><td colspan="2"><b>Assessment criteria</b></td><td><b>Included in answer</b></td></tr>
<tr><td rowspan="3">3</td><td rowspan="3">Understand how security can reduce risks in an organisation</td><td>3.1.</td><td>Explain the ‘preparedness cycle’</td><td></td></tr>
<tr><td>3.2.</td><td>Explain how the security function operationally supports other departments within the organisation</td><td></td></tr>
<tr><td>3.3.</td><td>Assess the importance of regular reviews of security plans and procedures</td><td></td></tr>
</table>

The Preparedness Cycle is a valuable tool for organizations that consists of five phases: mitigation, preparedness, prevention, response, and recovery. These phases represent a continuous cycle of activities such as planning, organizing, training, equipping, exercising, and evaluating emergency preparedness.

By implementing the Preparedness Cycle, organizations can enhance their overall capacity and resilience to effectively handle and recover from any kind of disaster. It enables organizations to develop comprehensive strategies and plans, ensuring their readiness for both natural and human-made disasters. While it may not be possible to prevent all disasters, proactive planning through the Preparedness Cycle can significantly reduce the risks to life and property during such events.

By implementing mitigation efforts, organizations can minimize the loss of life and physical assets, such as buildings and supplies, thereby reducing the overall impact of disasters on both organizations and communities. Prevention involves establishing solid plans, conducting training, and organizing exercises well in advance of disasters to prepare your organization.

Through engaging in emergency planning activities, organizations can decrease the loss of life and address environmental challenges by creating customized plans, standardized tools, and emergency management protocols. Preparedness includes a series of ongoing activities, such as emergency planning, staff training, drills, evaluations, and corrective measures. Preparedness and readiness are interconnected as organizations and communities prepare for potential disasters. Response refers to how organizations respond to the challenges posed by disasters, such as disruptions in the supply chain, changes in service delivery, or staffing issues.

When responding to disasters, organizations must effectively utilize their emergency preparedness resources, such as plans, policies, procedures, and staff training.

Recovery focuses on restoring critical business functions to stabilize day-to-day operations and enhance the ability to continue serving the community after a disaster. The recovery phase allows organizations to quickly return to normal service levels. Other Strategies for Emergency Preparedness: - It is important to conduct emergency preparedness activities throughout the year. - Emergency preparedness is an ongoing process of continuous improvement. - Identifying gaps in your emergency preparedness capabilities is crucial for enhancing your systems. Regularly scheduling emergency preparedness activities is essential. Emergency preparedness activities are essential for driving the preparedness cycle.

Workplace security usually covers various aspects such as physical security, information security, and ensuring the safety of employees.

Policies and procedures are often perceived as static and unchanging, but they should be adaptable to the evolving needs of your organization. Effective policies are not meant to gather dust on a shelf; they should be reviewed and updated regularly. If it has been a while since last examined security policies, might discover that they are outdated, no longer aligned with current laws and regulations, or fail to address the systems and technology your organization currently employs. Is considering the Information Security policies as the fundamental framework of security program, providing guidance to ensure that everyone in the organization understands their responsibilities in safeguarding data and assets.

Policies and procedures are essential components that provide a structured framework for organizations to function efficiently and effectively, ensuring consistency and compliance. Understanding their significance is key to achieving successful implementation.

Policies establish the rules, guidelines, and principles that govern decision-making and actions, while procedures offer detailed instructions on how specific tasks or processes should be carried out.

The significance of policies and procedures lies in their ability to offer structure, consistency, and transparency within an organization.

They ensure that all members are aligned, working towards common objectives, and following established protocols. Moreover, they help manage risks, ensure regulatory compliance, and foster a positive organizational culture.

Successfully implementing policies and procedures involves several key steps. This includes defining clear objectives, identifying stakeholders, developing comprehensive policies and procedures, providing effective communication and training, gaining support from all levels of the organization, and conducting regular monitoring and review for continuous improvement.

Regularly reviewing policies and procedures is an essential aspect of managing an organization. In an ever-changing landscape, where teams expand, expectations shift, and laws develop, it is crucial to conduct routine evaluations. By doing so, you ensure compliance and maintain effectiveness. Neglecting this practice is not a viable option.

Compliance Assurance: Consistent evaluations ensure that policies and procedures align with existing laws and regulations.

Risk Mitigation: Identifies and minimizes potential risks, safeguarding the organization against legal and financial complications.

Enhanced Operational Efficiency: Revisions optimize processes, enhancing the overall workflow and productivity.

Flexibility in Response to Change: Facilitates swift adaptation to evolving market conditions, technologies, and customer expectations.

Sustained Progress: Fosters a culture of continuous improvement and efficient feedback response.

Stringent Quality Assurance: Ensures the maintenance of exceptional standards in quality and service through regular assessment and enhancement of operational procedures.