

International Certificate in Security Management

Unit 2: Security Department 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: #1243-0823	437MIHA	
Is this a re-submission? <i>If yes please submit by email to office@ebssa.net.</i>	NO	
Word Count: <i>(This is the number of words that you have written in each task, and does not include your assignment title, diagrams/appendices or bibliography)</i>	Task 1:	921
	Task 2:	652
	Task 3:	824

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 plagiarism has been committed.

Signed: MIHAELA NITA

Dated: 15/03/2024



Module 2

Introduction to Security Department Management

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 2: Security Department Management

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

Task 1	<p>Explain the role of the security manager with reference to common tasks.</p> <p>Explain the different styles of and approaches to security management and which styles and approaches would you recommend.</p> <p>Explain what key methods you might use to communicate effectively within an organisation.</p> <p>Explain how security might be viewed within an organisation</p>	Guideline word count for Task 1 750
---------------	---	--

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 the role of security managers	1.1.	Explain the key aspects of the role of a security manager	
		1.2.	Explain the different styles of and approaches to security management	
4.	Know how to manage operations and physical resources	4.2.	Evaluate organisational communication techniques in relation to security operations	
		4.3.	Evaluate security operations within the organisation highlighting any issues or concerns	

Security managers are essential for maintaining the safety of staff and visitors in an organization. They are also responsible for ensuring that the buildings and locations they oversee are protected from any potential harm. Also are responsible for overseeing the security and safety of individuals working in a building and visitors to the site. They are typically seasoned security professionals with a strong background in public safety, who have advanced to a supervisory role. The specific duties of a security manager can vary depending on the size and type of the organization they are employed by, as well as the characteristics of the site they are tasked with safeguarding. Some common responsibilities of a security manager include supervising the security team, creating work schedules to meet security requirements, monitoring surveillance systems, conducting risk assessments, managing emergency responses, recruiting, and training staff, collaborating with law enforcement and security agencies, organizing security for special events, developing security protocols, investigating security incidents, and controlling access to restricted areas within the site.

Security managers are responsible for supervising the security team in their organization. The number of individuals they manage directly varies based on the company's size and security

Please ensure the full document is submitted for marking.

requirements, but all security managers utilize leadership abilities to a certain degree. This can involve delegating tasks efficiently, offering valuable feedback to subordinates, and creating and conducting training sessions for less experienced staff members.

Security managers oversee the comprehensive security of a location, conducting ongoing assessments to prevent security breaches and ensure safety. Their keen attention to detail enables them to promptly identify any irregularities that may pose a threat.

Security managers often interact with members of the public, such as colleagues, visitors, or guests. While security is not primarily a customer service role, possessing strong customer service skills can aid security managers in handling conversations with the public more effectively. If you aspire to become a security manager, you can start by honing transferable skills like verbal communication. Security managers may utilize various software and computer programs to carry out their responsibilities. This could involve programs enabling quick communication with coworkers, or software related to monitoring CCTV cameras and alarms within the premises. Therefore, security managers must possess at least basic computer literacy to execute their duties efficiently. Developing the ability to evaluate your performance and accept constructive criticism without becoming defensive is a valuable skill for any profession. This skill is especially crucial for security managers, as any lapse in their standards or performance could pose serious risks to public safety. Hence, security managers consistently evaluate their own performance as well as that of their team.

Nowadays, there are unpredictable changes and advancements occurring in social, economic, and technological sectors. These changes not only enhance the convenience of individuals' lives but also introduce new risks. The improved communication network resulting from technological progress offers easy information access, yet it also opens doors to security breaches. Consequently, as changes take place in various areas, adjustments in security services provision and management are also necessary. It is crucial that modifications in security management are implemented promptly, efficiently, and precisely.

The concept of security, which is one of the most fundamental human needs, has always been in high demand throughout history. As individuals and societies have undergone various changes, the nature of security has also evolved and diversified. While physical security was paramount in ancient times, today the protection of intangible assets holds equal importance. Take the security of a nation, for instance. Moreover, with technological advancements and the rise of globalization, the world has become a closely connected global community. This has significantly transformed the concept of security, necessitating a shift in security management practices to meet the expectations of individuals and society.

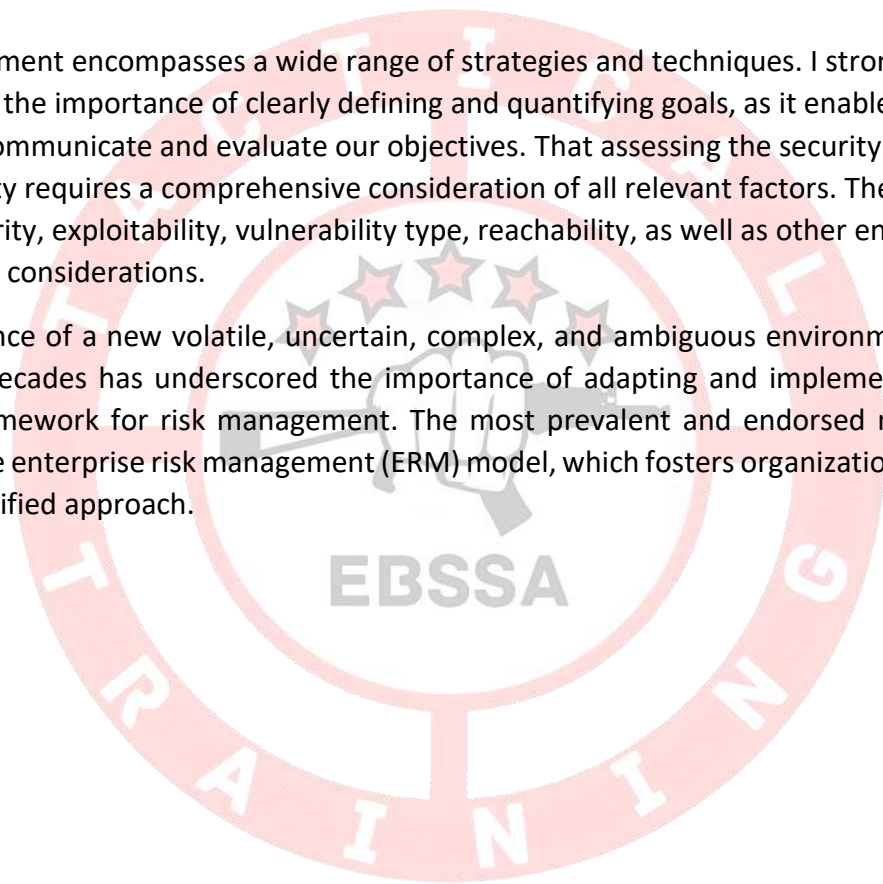
The concept of management involves the dynamic process of planning, organizing, directing, coordinating, and supervising activities. Security management, on the other hand, focuses on eliminating threats and protecting individuals, organizations, and states from risks and dangers. Just like management, security management is subject to changes over time, influenced by social demands and environmental factors. Various theories and models have been proposed to adapt management mechanisms to these changes.

The COBR Strategic Coordinating group consists of Gold Commanders from various representative groups, each of which includes organizations with their own Gold Commanders. This system effectively brings together a wealth of information and expertise in a single meeting, enabling rapid and efficient dissemination of orders and requests throughout the command structure.

The GSB system offers the advantage of enabling Bronze Commanders, Silver Commanders, and Gold Commanders to collaborate with commanders of similar levels in different systems. This facilitates the formation of highly efficient multi-team working groups. It is specifically designed for government-level crisis management, allowing for the coordination of numerous organizations during national crises such as terrorism, health scares, or natural disasters like flooding.

Risk management encompasses a wide range of strategies and techniques. I strongly advocate for the importance of clearly defining and quantifying goals, as it enables us to effectively communicate and evaluate our objectives. That assessing the security risk level of a vulnerability requires a comprehensive consideration of all relevant factors. These factors include severity, exploitability, vulnerability type, reachability, as well as other environmental and business considerations.

The emergence of a new volatile, uncertain, complex, and ambiguous environment over the past three decades has underscored the importance of adapting and implementing a fresh strategic framework for risk management. The most prevalent and endorsed model in this context is the enterprise risk management (ERM) model, which fosters organizational resilience through a unified approach.



Task 2		<p>Explain how you would make a commercial case for budget spend and what areas would you cover.</p> <p>Explain the key areas of security expenditure you might be called upon to manage.</p> <p>Define legislation relating to financial transactions that the security manager might have to be aware of</p>	<p>Guideline word count for Task 2</p> <p>500</p>	
<p><i>Task 2 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></p>				
Outcomes of learning		Assessment criteria		Included in answer
Understand the financial control aspects of the security management role	2.1.	Explain how to prepare a commercial case for a security management budget spend		
	2.2.	Explain how to manage financial expenditure		
	2.3.	Define the legal requirements regulating financial transactions		

The business case is crafted in the initial phases of a project and provides a comprehensive overview of the reasons, objectives, approach, and stakeholders involved in determining the viability of proceeding with the project.

Key components of the business case include:

1. Business vision: Clearly articulating the long-term goals and aspirations of the organization.
2. Business need: Identifying the specific problem or opportunity that the project aims to address.
3. Expected benefits: Outlining the anticipated advantages and outcomes that the project is expected to deliver.
4. Strategic fit: Assessing how well the project aligns with the overall strategic objectives of the organization.
5. Products produced: Describing the tangible deliverables or outcomes that will be generated by the project.
6. Broad estimates of time and cost: Providing high-level estimates of the time and financial resources required for the project.
7. Impact on the organization: Evaluating the potential effects and implications of the project on the organization.
8. Risks: Identifying and analysing the potential risks and uncertainties associated with the project.
9. Costs, including investment appraisal: Assessing the financial implications of the project, including the return on investment.

10. Technical solutions: Describing the technical approaches and solutions that will be employed to achieve the project objectives.
11. Timescale: Establishing the projected timeline for the project, including key milestones and deliverables.
12. Impact on operations: Evaluating how the project will impact the day-to-day operations of the organization.
13. Organizational capability to deliver the project outcomes: Assessing the organization's capacity and resources to successfully execute the project.

In addition to these components, the business case also includes an executive summary, financial considerations, project definition, and project organization details. These elements provide a comprehensive overview of the project and enable stakeholders to make informed decisions regarding its continuation.

As a manager, the ability to adhere to a budget is a critical factor in the performance evaluation. It is essential for every department within an organization to stay within their allocated budget to achieve the desired profit margins. Overspending directly impacts the profit, but under-spending can also be detrimental as it ties up funds that could have been utilized more effectively elsewhere.

It is crucial to constantly monitor the spending in comparison to the budget to avoid any financial surprises later in the year. Neglecting to pay attention to the budget early on can lead to financial constraints in the later months.

Effective budget management consists of two key elements:

1. Planning – accurately estimating and negotiating a reasonable budget.
2. Discipline – committing to operating within the budget by reallocating funds when necessary.

Successfully managing a budget not only benefits the organization but also enhances the professional reputation. Therefore, it is imperative to establish a precise budget from the beginning and devise strategies to overcome any challenges that may arise.

The initial step in budget management involves the process of sitting down and determining the exact amount of money required to accomplish the objectives. Nowadays, the organizations must operate in a streamlined and efficient manner, with every dollar being meticulously tracked and allocated.

While it is possible to use previous budgets as a reference point, the most effective approach is known as "zero-based budgeting." This method entails starting with a blank budget and justifying each dollar that is planning to spend.

Legal requirements regulating financial transactions (Data Protection 1998, like a part of CCTV, store information and personal data. Wireless and Lan increases de risk information. A securities financing transaction encompasses various types, such as a repurchase transaction

where a security is sold with an agreement to repurchase it in the future, including an additional return for the use of the funds. It may also encompass the act of loaning a security for a fee, in return for a guarantee offered by the borrower in the form of financial instruments or cash. Furthermore, it could encompass transactions such as buy-sell back or sell-buy back, along with margin lending transactions.

Task 3		Describe what leadership is and identify any 3 theories of motivation the security manager might use. Explain what management is and identify any 3 recruitment and management skills. Explain what a service level agreement is and why they are important when dealing with external providers		Guideline word count for Task 3 750
<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>				
Outcomes of learning		Assessment criteria		Included in answer
3	Know how to manage security personnel	3.1.	Describe the requirements of leadership and principles of motivation in relation to managing security personnel	
		3.2.	Describe the skills required to recruit and manage security personnel	
4	Know how to manage operations and physical resources	4.1.	Explain the importance of having Service Level Agreements with internal and external providers	

The influence within the formal company hierarchy as a senior member of management depends heavily on the credibility can establish with the leadership. It is essential to feel confident in rightful place among other managers of similar rank during management meetings. To achieve this, must demonstrate both sector-specific expertise as a security professional and be adept in the role as a senior manager involved in executive decision-making. Security managers should be mindful of these key points when participating in executive meetings:

Motivation theory delves into the underlying factors that propel individuals to strive for a specific goal. Instead of viewing motivation as a mysterious trait unique to each person, motivation theories provide a structured foundation based on research to comprehend the precise drivers that compel individuals to progress.

Motivation theory examines the various factors that prompt individuals to work towards a specific objective. Instead of perceiving motivation as an enigmatic quality exclusive to individuals, motivation theories present an evidence-based framework to comprehend the specific stimuli that impel individuals towards advancement.

Maslow's theory initially centered on the basic needs of individuals, but over the years, it has been frequently modified and implemented in professional settings.

Prominent organizations recognize the significance of collecting feedback from their employees during the implementation of changes. Who could provide leaders with more valuable insights regarding the potential impact of organizational strategies and initiatives than those directly involved. Employees possess firsthand expertise in their roles and are frequently highly perceptive about the necessary modifications required to attain superior outcomes for the organization.

1. Organizations can utilize employee opinion surveys to uncover and tackle obstacles that hinder productivity and efficiency.
2. Employee opinion surveys provide valuable insights into employee comprehension and perspectives regarding policies and human resources programs.
3. By conducting employee opinion surveys, organizations can pinpoint the incentives, bonuses, special assignments, time off with pay, training and development, and flexible work schedules that are most appealing to their employees.
4. Employee opinion surveys help identify gaps in training and development, allowing organizations to determine the areas in which additional training is needed.
5. Through employee opinion surveys, organizations can identify areas of communication breakdown and team conflict, enabling them to take effective measures to address these issues.
6. Employee opinion surveys serve as a predictive tool, helping organizations anticipate and understand employee responses to organizational change.
7. By conducting employee opinion surveys, organizations can uncover the underlying sources of morale and turnover problems, allowing them to implement targeted interventions to address these issues.

Clear and assertive communication plays a crucial role in the security field. Security managers need to effectively communicate with individuals from diverse backgrounds. Whether they are interacting with visitors, employees, or stakeholders, it is vital to convey instructions, explain security procedures. Possessing the capability to observe and uphold situational awareness is an essential skill for security managers. Cultivating a sharp sense of observation entails being vigilant towards intricate details, discerning suspicious conduct, and pinpointing potential risk and share necessary information in a concise and understandable manner.

Security manager must possess the necessary skills to effectively handle conflicts as they often encounter challenging and potentially unstable situations. By mastering conflict resolution techniques, they can defuse tense scenarios and prevent further escalation. Moreover, their ability to restore order after de-escalation is crucial.

A personnel security specialist must possess a diverse set of hard skills. Proficiency in JPAS, E-QIP, and DoD is essential, along with experience in personnel security, security policies, background checks, and investigative reports. Additionally, familiarity with working alongside government agencies is necessary. Moreover, they should be capable of providing administrative support and performing data entry.

Soft skills are equally vital for a personnel security specialist. They should excel in collaborating with law enforcement to ensure the development and consideration of all pertinent information in alignment with security policies and regulations. Furthermore, they should be adept at working harmoniously with both external and internal customers/security staff, all while upholding the utmost standards of professionalism and integrity.

An SLA, also known as a service level agreement, is a comprehensive contract or agreement between a company and its service provider. It outlines the specific expectations and responsibilities of both parties involved in the business relationship. Collaborating with a service provider offers numerous benefits, however, to ensure optimal outcomes, it is crucial to establish an SLA.

SLAs include responsibilities that both the vendor and customer must meet throughout the duration of the SLA for agreements to be legally binding. Failure to meet these responsibilities can result in claims of SLA violations, enabling customers to enforce their right to receive penalty fees from the vendor.

Establishing a Service Level Agreement (SLA) can prove advantageous for both prospective clients seeking managed services and service providers. By identifying key components to include in the agreement and setting transparent expectations early in the client/partner relationship, is possible to prioritize the company's interests and enhance the overall value of the business partnerships.