Transcript 6

Welcome to this video presentation (slides with voiceover), on an introduction to Risk Management Fundamentals. Having established last week that there is an essential need to have security and risk management due to the increasing amount of threats and attacks, we will now look into more detail with regard to what this entails. This week we will discover other essential areas to cover in order to gain a greater understanding of managing security and risk in a digital environment.	Intro slide
We will now take a look at what Darril Gibson (author of the core text for the module), claims regarding risk management fundamentals. He states that *"Risk management tis important to the success of every company",* and that failure will occur if this is not carried out adequately. He also claims that effective risk management starts by gaining an understanding of both threats and vulnerabilities and the importance of identifying ways to mitigate risk if we are to succeed in successful management in this field.	Slide 2
We will now take a look at what the essentials are to start the process of risk management. We should begin the process with a risk assessment and evaluation as well as applying metrics for identifying any risks. We see in this slide that Risk equals: • the possibility of financial loss • uncertainty • threat x vulnerability and that • total risk is equal to threat x vulnerability x asset value. We saw last week that Assets are anything that has value to an individual or an organisation. These assets need to be protected from all types of attacks and misuse; from illicit access, use disclosure, alteration, destruction, and/or theft – all that can result in a loss to an organisation or individual. We will look at assets in greater detail further on in the module.	Slide 3
We continue with defining 'Threats', 'Vulnerability' and 'Loss'. Threats are any activities that are a possible danger; a human-caused or natural event that could impact a system. Vulnerability is a possible weakness in a system that can be exploited, and finally 'Loss' results in a compromise to the business functions or assets. We now know that threats and vulnerabilities are the key drivers of risk (the likelihood or probability of an event and its impact), and they need to be identified in order to take relevant and adequate action to reduce potential losses from these risks. There are no actions without decisions as information gives us power to make informed decisions. It is essential that the right decisions are made in this field. The decisions whether or not to mitigate risks for example.	Slide 4

In the process of security and risk management, the key and first step to take is to identify any threats and vulnerabilities as these can then help to determine the severity of the risk and therefore the relevant action can be taken.	Slide 5

Risks can then be managed by choosing one of four techniques that can be applied where a risk can be: • avoided • shared or transferred □ mitigated □ or accepted. Risk mitigation is the primary technique, related to risk reduction or risk treatment whereby vulnerabilities are reduced by implementing controls or countermeasures to address the issues.	
Now, please pause/stop the video before continuing to listen to the rest of the lecture, and let us now take a short break and reflect what we have learned so far before continuing with the lecture and looking at elements of risk management. What are the essentials to be considered in risk management, and what is needed in order for effective risk management can be carried out?	Slide 6
Welcome back after taking that break, we can now continue with looking at elements of risk management. In this slide, we are given a list of elements of risk management with the aim to assess risks by using risk assessments or risk analysis. We need to identify the organisation's IT assets and their subsequent value and this might include data, hardware, software, services, and the IT infrastructure. These elements also include the identification and prioritisation of threats and vulnerabilities. It is essential to ascertain the probability that a vulnerability will be possibly exploited by a threat and the levels of probability, and these are the risks. The impact of a risk should also be identified and of course prioritise risks with a higher impact.	Slide 7
Continuing on with elements of risk management, we have to identify risks that are to be managed and this is where careful decision making is required. To adequately address the risks, decisions have to be made by choosing to either avoid, share, transfer, mitigate or accept the risks. Once the decisions have been made, controls/countermeasures for these chosen risks have to be selected. These countermeasures are introduced to focus on reducing vulnerabilities and their consequent impact.	Slide 8
In order to ensure relevant protection for these risks, countermeasures need to be implemented and tested to ensure their validity. They should also be evaluated on a regular basis to ensure necessary protection is implemented. Other elements to be considered are the costs incurred to manage risks as these have to be balanced against impact value. In other words, they should be cost effective with regard to asset loss. Financial cost of risk management rarely adds profit!	Slide 9

So in order to manage security and risk, what are the essential management skills needed to do so? In the next two slides, we will see lists of these essential management skills as identified by Bruce Newsom. We need to understand, analyse and assess security and risk and know what they mean. We need to understand and analyse the sources of risk to also include the hazards, threats, and contributors of these.	Slide 10
We should also understand and analyse the potential targets by their exposure and vulnerability as well as understand and assess uncertainty and probability, and levels of the probability. Understanding and assessing the potential reoccurrence of an event are also essential to ensure adequate countermeasures are in place. A skill is also needed to develop an organisation's culture structure, and processes congruent with better security and risk management infrastructures.	
Continuing on with essential skills, we need to establish risk sensitivity and tolerability in order to understand the difference between 'real risk' and 'perceived risk', as these can impose unnecessary costs. Risk needs to be controlled and the ability to select different strategies for managing risks is essential. The competence to record, communicate, review, and audit risk management, and improve security in primary domains, including operation and logistics, is needed. The knowledge of physical sites and information, communications and cyber space as well as personal security is essential.	Slide 11
Here, we visit the C-I-A Triad, this forms the basis of information security and is comprised of three fundamental information security concepts. **Confidentiality**: this is the prevention of unauthorised access or disclosure of information. An example of loss of confidentiality is where passwords, or an organisations' confidential information is exposed. **Integrity**: safeguards the accuracy of information and processing methods. It prevents unauthorised users or processes from making any alterations/modifications to data. Examples of loss of integrity are emails that are modified in transit, viruses, and personnel making unauthorised changes to a Web site. **Availability**: is where reliable and timely access to information and associated systems and assets when needed, are ensured. Examples of loss of availability is where file and email servers are down, and there is a lack of access to them.	Slide 12
In summary, the preceding slides are an overview of risk management fundamentals where we have been introduced to Risk, Vulnerability, Loss etc and their identification. We have also been introduced to elements of risk management as well as essential skills and risk identification techniques. The references used in this lecture are: 1. Gibson, Darril., (2020), *Managing Risk in Information Systems.* 3rd ed. Jones and Bartlett. 2. Newsom, B., (2014), *A practical introduction to Security and risk Management.*	Slide 13

Now take a break and reflect on what we have learned so far before moving on to the next task for the week. Your next task is to read Chapter 1 of the core text which will enable you to gain a more in-depth understanding of the fundamentals of risk management to extend your knowledge and understanding of the subjects raised in the lecture.	