# Business Continuity Plans

Welcome to this lecture slides with voiceover on Business Continuity Plans (BCP). We have seen in previous lectures the importance of establishing security within the organisation and the first step is the development of written policies covering all the aspects of security. These policies form the documentation for Business Continuity Planning (BCP) as well as Disaster Recovery Planning (DRP). These two plans work alongside each other but involve different activities.

A BCP is a plan that keeps the business running after the occurrence of a disaster, and a DRP is concerned with restoring business operations after the said disaster. We will be looking at disaster recovery planning in the next lecture. To ensure effective security management commitment has to be made to understanding and forcing and following these policies. It is important that there is an awareness of these policies and procedures, as well as supporting explanations to ensure they are correctly understood. They should be readily available for all employees in the organisation.

It is of no use just having these policies as it is essential to read them, understand them and enforce them.

So let us firstly look at how we might define business continuity. According to Gibson and Igonor, a business plan "is a plan designed to help an organisation continue to operate during and after a disruption... the goal is a continuation of operations". It is ensuring business operations can continue in an emergency and creating policies, plans and procedures to minimise the impacts of risks. These risks may be due to intentional attacks, unintended attacks, failures as well as natural disasters. The scope of the BCP includes a global view of the organisation where it looks at all the elements, but does not mean that all the elements of the organisation need to continue to operate. Elements that are mission critical are the ones that are essential and need to continue to operate. Therefore, these are the ones to be focussed on.

A BCP involves creating plans to ensure that the business can maintain continuous operations in the event of an emergency. There are four main steps: project's scope and planning, business impact assessment, continuity planning and approval and implementation. We will look at these individually. Project scope and planning. This needs analysing from a crises management perspective, and the first stage is to create a BCP team with senior management approval to assess any resources available and analyse legal and regulatory requirements. These will depend on the company's size and infrastructure. The steps taken are as follows. These will include the departments that provide critical operations, critical support services, the IT and maintenance team, the department responsible for physical security of the organisation. This process is carried out for a second time to ensure that the key areas of business are not overlooked. input from the organisational level to ensure the communication of the plan. The Business Impact Assessment BIA, this assessment involves identifying the priorities previously highlighted by the BCP team as well as any risks. This assessment includes the probability of a threat occurring and the impact it might have on the business. Continuity planning: this involves strategy development, provisions and processes, people, buildings and facilities, as well as infrastructure and the possibility of alternative systems. The plan will contain planning contingency events. Some risks will be too complex to justify, and this needs to be fully documented. The plan must also ensure that people in the organisation are protected before and after the crises has occurred, and the building and facilities will include ensuring these. There may be alternative sites needed where operations might continue. This plan will also include a disaster recovery plan that might include discovering and overcoming potential weaknesses, such as implementing computer, say, fire suppression systems or even putting an alternative system in place. Approval and implementation: this plan has to be approved at the executive level first and foremost and staff training should then be carried out to ensure the smooth running of the operations. The plan should be regularly updated and tested to ensure it is fit for purpose. This includes training people, ensuring they understand the details of the BCP, testing in order to verify that the BCP will function as planned and deploy exercises demonstrating how the BCP will work.

Policies and procedures in a business continuity plan include reviews of existing risk assessments and the business impact assessment that we have seen in the previous slide is the initial step in a business continuity plan. According to Johnson, the purpose of BIA is to identify critical processes and assess the impact of a disruptive event, and it can identify any control weaknesses in the operations. Johnson provides a list of the outcomes from a BIA that include the following: a list of critical processes and dependencies, a workflow of processes that include human requirements for recovering key assets, an analysis of legal and regulatory requirements. A list of critical vendors and support agreements and an estimate of the maximum allowable downtime. This means assessing the amount of time available before normal functions and operations are retrievable. The Business Continuity Plan is based and relies on the findings of the business impact analysis. Business impact analysis assesses the most resilient and most fragile process of the business. This might include a vulnerability test to determine the quantitative and qualitative impact of the loss of a business function, and we have now seen how quantitative and qualitative process are carried out in previous lectures. It is important to assess and estimate the complexity and how long the disaster will affect the critical business functions and consequently the impairment incurred. The timing of the disaster is important as it might occur at the busiest time in the business cycle, and this consequently affects the impact it has. Recovery targets have to be established from the time the disaster occurs to when normal functions and operations can continue. Another consideration is the response and recovery time objectives (RTO) which relates to the time a business process must be restored after a disaster. This relates to the business processes and not the technology. It is a metric for seeing how quickly business processes can be recovered.

To summarise, the main purpose of a BCP is to ensure mission critical systems such as functions and processes and operations that keep the organisation running are identified after a disruption of operations. This plan will then be implemented until normal operations are resumed. Part of this plan includes a business impact analysis that consists of identifying critical business functions, that is any function considered vital to an organisation. Also identifying critical processes that support the critical business functions (CBFs). IT services supporting the CBF should be identified, as well as determining acceptable downtime for CBFs processes and IT service. The BCP also includes maintenance plans, where the plan is regularly reviewed, tested and updated, and looks at any changes to the IT infrastructure.

In this lecture, we have had an introduction and overview of a business continuity plan. The following task is to read chapter 13 of the core module text, which will give you detailed information regarding the BCP and supplement this lecture. Now take a break before moving on to the next task.