Security Governance and Compliance Transcript

Security Governance and Compliance Transcript

Welcome to this video presentation (slides with voiceover), on security governance and compliance.

It is important to understand the roles that governance and compliance play in ensuring the security of an organisation and what these roles entail. We have looked at a number of laws and regulations for the protection of IT systems and the challenge is the issue of compliance with them. This lecture will look at some of the security administration policies, procedures and regulations that are needed, and the importance that knowledge and understanding of these is essential in order for governance and compliance to take place within the organisation.

We will begin the lecture by looking at definitions of governance and compliance.

Governance is a set of specific actions that are taken to ensure the organisation complies with its policies, processes, standards, and guidelines, with the ultimate goal of meeting the business requirements. It is essential that there is a good understanding of the business itself as well as its objectives, and the focus and challenge is that everyone in the organisation should comply. Good governance is where assurance and confidence that rules are being correctly understood and followed. Quality assurance and quality control should be embedded, and are part of the effective governance promoting awareness and providing evidence of security control. The governance process in an organisation is usually assessed, and these assessments can be self-assessment, internal audits, or regulatory reviews where operational risk or compliance functions within the organisation may perform a review. Evidence of governance can be seen in the configuration management process where mitigated vulnerabilities remain in check. Configuration management is the process of identifying, controlling, accounting for, and auditing changes made to a preestablished baseline. It is a formal process that controls changes to systems. Change management is important to use with basic security activities. Quality assurance and control are part of the change management process and quality assurance governance routines, review and approve any changes. (1)

Compliance is to do with individuals and an organisations levels of compliance with security policies. It is common practice to implement policies in an organisation to ensure they are compliant with different laws and regulations. Metrics for security compliance is complex, however, they might be measured against security controls relevant to **how** information is protected, or security policies, **why** you set the goal, and this bridges business requirements with security control. Lack of compliance can result in not only risks, but it can also incur fines and offences when not complying or adhering to laws and regulations, also resulting in a possible prison sentence.

Security Governance and Compliance Transcript

We continue with defining security governance, this is a definition by NIST: *'How organisations can control, direct, and communicate their cyber security risk management activities'.* We know that it is important to test against policies and procedures to ensure compliance is maintained within the organisation. Governance is a means for the organisation to communicate their risk management activities. Security governance is to take control of the cyber security risk and much depends on the size and the complexity of the IT infrastructure within the organisation; the available resources, and other external variables. IT governance includes standards, processes and activities to ensure the security against cyber risks.

This slide shows us a set of security governance principles:

- It is comprised of a collection of practices to support, define, and direct security in an organisation
- It is related to corporate governance and IT governance
- Security is not just an IT issue
- Governance affects everyone and everything in an organisation
- Security is a business operations issue

The first diagram on this slide depicts the Bottom Up approach to secure security planning. Here we see that it is the IT department making the decisions regarding security of the organisation without the inclusion of senior management. This can be problematic for a number of issues and that is why this approach is not usually deployed.

The right hand diagram shows the management planning using the Top Down approach where senior management define the security policies providing direction for security measures to be implemented within the organisation. Middle management use these polices from senior management to provide standards, guidance, and procedures, in line with the policies. Operational management of the security teams use this information to provide practices and configurations, and at the bottom of the diagram we see the end users who have to comply with these practices to ensure the security of the organisation. These approaches can provide organisational wide compliance.

Security Governance and Compliance Transcript

When applying security governance principles, there are three plans that can assist; strategic, tactical, and operational plans. A strategic plan is a long term plan that tends to be robust and defines the organisation's security purpose. This approach also helps to understand security function and align it to the goals, mission, and objectives of the organisation. A strategic plan has a useful life for approximately five years if it is regularly maintained and updated annually. It also serves as the planning horizon, where long term goals and visions for the future are discussed in a strategic plan. A strategic plan should also include a risk assessment.

A tactical plan is a mid-term plan and is developed to provide more details on achieving the goals set out in the strategic plan. This plan can be ad-hoc based upon unpredicted events and it is typically useful for approximately one year. The tactical plan often prescribes and schedules tasks that are needed to achieve the organisational goals.

Finally, an operational plan tends to be short term and highly detailed, and based on the two previous plans – the strategic and tactical plans. This is only valid or of any use for a short length of time. It is essential that operational plans are updated frequently and they must include details on how the implementation processes are in compliance with the security policy for the organisation.

At the beginning of the lecture, we introduced Change Control management and this is essential as we know that change can impose new security vulnerabilities. Security can only be maintained when changes are necessary, by systematically managing it. The change control usually involves extensive planning, testing, logging, auditing, and monitoring.

In order to be effective, changes have to be implemented in a monitored and orderly process. Formalised testing is included to verify that a change produces the expected results. Changes can be reversed by applying 'backout' or 'rollback' plans and procedures. Changes are communicated to users before they are implemented to prevent loss of productivity, and the effects of the changes are systematically analysed to ensure quality. By implementing change control procedures, negative impacts due to changes on capabilities, functionality, and performance, are reduced. There is a changes review and approval process that is carried out by a Change Approval Board (CAB).

To conclude: we know that policies define the scope of the organisations security and the assets owned that need protecting. Policies are an overview of the security needs that provide high level strategic planning outlining security goals of the organisation. Standards are mandatory and define the specifics of the policies. Procedures are also mandatory and provide step by step instructions on how things should be carried out. Guidelines on the other hand are not mandatory, but they show how things should be carried out and highlight best practices.

Take a break and reflect on what we have learned so far before moving on to the next task for the week.