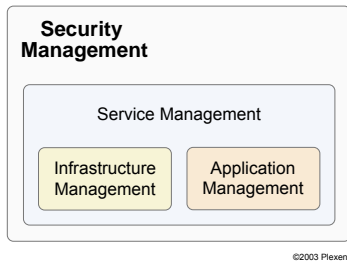


What is Security Management?

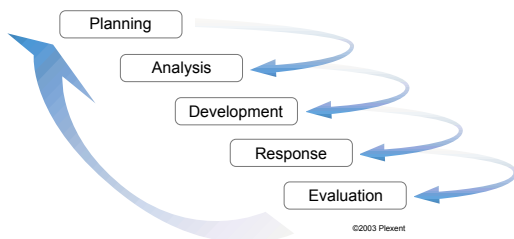
ITIL defines Security Management as:

... the process of managing a defined level of security on information and IT services... [and] managing the reaction to security incidents.

Security Management is often shown as a separate process, distinct from the Disciplines that make up Service Delivery and Service support. In this sense ITIL treats Security Management as external to, but supportive of, the Service Management core. Plexent believes that Security Management is better visualized as surrounding and protecting the core, providing a backdrop against which the other Disciplines operate and a context in which they should be evaluated. This concept is illustrated below.



At the highest level, Security Management impacts all Disciplines and should be reflected in the levels of confidentiality, integrity, and availability required within the Service Level Agreements (SLAs) and Operational Level Agreements (OLAs) under Service Level Management. At a lower level, there is a close kinship between Security and Continuity Management in that each relies heavily on the tools and techniques of risk management. This reliance can be seen by reviewing the activities necessary to implement Security Management as shown in the diagram below.



Security begins with Planning. Here the organization must examine business needs and its own culture to make an objective determination about collective risk tolerance. It is important for an organization to know at the outset if they are generally risk averse, neutral, or risk seeking as this will strongly suggest which strategies should be considered. Next, Analysis involves both qualitative and quantitative techniques to evaluate what assets to protect from which internal or external threats. Here risk is broken down to its components so the probability and impact for each event can be evaluated. Development then seeks to offset the inherent lack of control and information through the creation of specific responses based on organizational risk tolerance and the following preferred approaches: Accept, avoid, mitigate, or transfer. When triggered by a security event, these strategies are executed in accordance with the tasks detailed under Response. Finally, periodic program review, as well as feedback regarding the suitability and effectiveness of actions under Response, must be provided to Planning to ensure relevance and continuous improvement.

The Plexent Approach

itDNA builds on the Security Management concepts outlined in the ITIL standard and, by leveraging our framework, Plexent can apply ITIL to your organization. If you are just getting started with Security Management you may need help setting up a convenient classification scheme to use under qualitative analysis. Or perhaps IT is not a core competency in your organization and you need assistance understanding the threats, such as address spoofing or packet sniffing. Or maybe IT is a core competency but you simply lack the resources to investigate, plan and implement a comprehensive access control solution. Whatever your Security Management maturity, Plexent can take you to the next level by bringing all of the pieces together.

Much more than just a framework, itDNA brings real-world tools and techniques to bear on your concerns. Backed up by itDNA's maturity models and rich, intellectual property knowledge base, Plexent's project management combines with proven policies and procedures to provide standardized services within the following Security Management Elements:

- Monitoring
- Security Development
- Access Control

When employed in concert with a Service Improvement Program (SIP), Security Management can actually help transform your corporate culture. This is true because security begins and ends with the people in your organization. When allowed to permeate your organization, Security Management reinforces a propensity for planning, attention to detail, and the habit of best practices. Understanding that people are at the heart of your security program underscores the need to hold their attention, encourage their involvement, and obtain a level of commitment necessary for Security Management to be successful. This can be easily accomplished through a program of security awareness, education and training.

Other benefits of a mature Security Management program include:

- Overall increased level of security
- Data loss prevention
- Data integrity assurance
- Guaranteed confidentiality
- Statutory and regulatory compliance
- Increased customer confidence
- Heightened employee awareness

If Information is the lifeblood of your business then Security Management is just the tonic for keeping the IT services that rely on it and the heart that pumps it, strong and healthy. By surrounding and protecting the Disciplines within Service Delivery and Service Support, Security Management contributes to the overall effectiveness of your Service Management Program. Can you get along without Security Management? Of course... to the same extent you can handle the increased cost and decreased productivity associated with immaturity in any of the other Disciplines. The question is, why would you want to? To help you evaluate where your organization stands with Security Management, Plexent provides assessment services. Leveraging the intelligence in our itDNA, we can help you evaluate where you are today, where you would like to take your organization, and the surest path to get there.

® ITIL is a registered trademark of OGC.