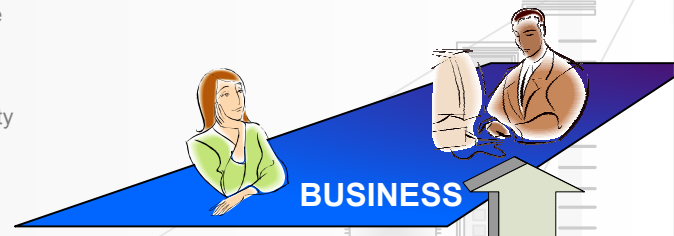
This flow chart has a specific process focus, but also indicates where other processes contribute.

Reviewing and/or compliance with the International Standard *"ISO 17799, Information Technology – Security Techniques"* provides necessary guidance on the entire topic of Security Management



Security Management Process

The Confidentiality, Integrity and Availability concepts are easily understood by non-IT (Business users). Ideally, the level of information security required should be derived from these business users and described in these three terms.

The "**value**" of information

Only authorized access

Accuracy and completeness

Timely availability

TRANSLATION

Confidentiality | Integrity | Availability

Gathering Security Requirements need not be conducted as a separate exercise. It can be part of understanding the Service Level Requirements of the customer (part of Service Level Management)

Negotiation of security requirements regarding services delivered

SERVICE PROVIDER

The concepts discussed here apply equally if an organization has fully outsourced the provision of its IT Services.

The Information Security Manager faces the continual challenge of limitless potential security challenges vs. the cost of protecting against those challenges.

The Security Policy

The Security Policy will explain the requirements for organizational security. It is important that the Information Security Policy supports the overall organizational security policy.
The organizational security policy may document issues like criminal history checks – such items cannot be countered in the Information Security Policy.

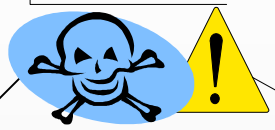
The "**protection**" of information

MANAGING RISKS

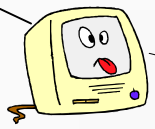
Security Controls

Controls can take a variety of forms. These include; Roles and responsibilities - Security Management, Security review team, specialist analysts.
Security Audits – Internal & external
Specialist purchases – specific security protection systems (physical, technical)

Managing Security Incidents

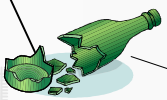


Sometimes a security issue can be obvious and easy to see. We can call these "threats". We can also learn from others about the types of threats they face. We may choose to refer to these as "warnings".



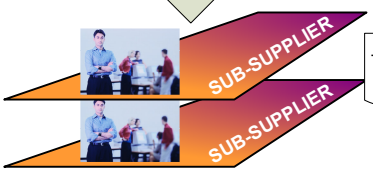
Despite our understanding of threats and warnings – there will be occasions that an actual security incident occurs. At such time we need to have in place mechanisms for identifying, reporting, recording and managing such incidents. These security incidents can follow a common incident management process or a specialized procedure.

External organizations



When a security incident occurs there is a high chance that some damage will have occurred. This fact needs to be recognized and built in to the security policy. Corrective measures to allow damage to be fixed may include restoration from backup, fail over to an alternative site or recalculation of data using algorithms.

MANAGING RISKS



The Security Policy | External organizations | Managing Security Incidents | Security Controls

The entire security management policy will flow on to our external providers. Ideally, we would look for evidence of their protection systems that support our own.

Important note: Internationally recognized flowchart symbols are used when their use is unambiguous

Decision | Predefined process | Document | Stored Data | Manual Operation

This flow chart prepared by The Art of Service as a representative example. Errors and Omissions Excepted