security planning

Security planning considers how security risk management practices are designed, implemented, monitored, reviewed and continually improved.

Entities must develop a security plan that sets out how they will manage their security risks and how security aligns with their priorities and objectives.

The plan must include scalable control measures to respond to increases or decreases in risk when a threat to the entity changes.

Risk Analysis

A security risk is something that could cause harm to people or that exposes information or assets to compromise, loss, unavailability or damage.

Shared security risks are risks that extend across:

- entities
- premises
- the community
- industry
- international partners
- other jurisdictions.

Stakeholders must cooperate to effectively understand and manage shared risks.

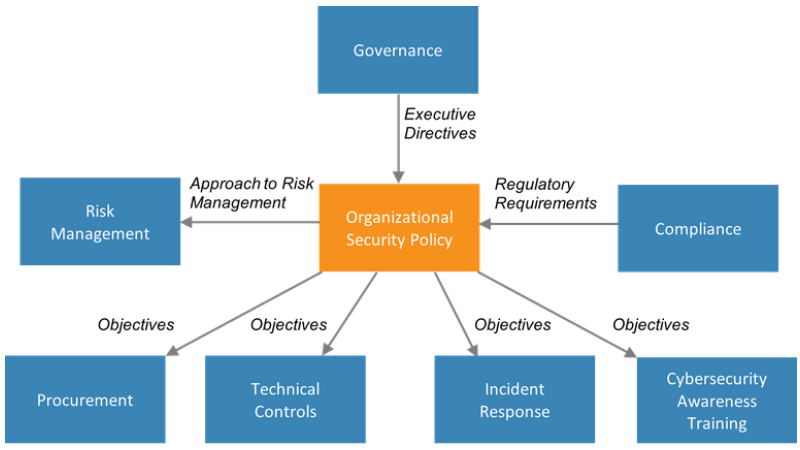
Entities must identify a risk steward (or manager) who is responsible for each security risk or category of security risk.

The 4 steps of a successful security risk assessment model

1. **Identification**. Determine all critical assets of the technology infrastructure. Next, diagnose sensitive data that is created, stored, or transmitted by these assets. Create a risk profile for each.
2. **Assessment**. Administer an approach to assess the identified security risks for critical assets. After careful evaluation and assessment, determine how to effectively and efficiently allocate time and resources towards risk mitigation. The assessment approach or methodology must analyze the correlation between assets, threats, vulnerabilities, and mitigating controls.
3. **Mitigation**. Define a mitigation approach and enforce security controls for each risk.
4. **Prevention**. Implement tools and processes to minimize threats and vulnerabilities from occurring in your firm's resources.

Organizational Security Policy

The *organizational security policy* is the document that defines the scope of a utility's cybersecurity efforts. It serves as the repository for decisions and information generated by other building blocks and a guide for making future cybersecurity decisions. The organizational security policy should include information on goals, responsibilities, structure of the security program, compliance, and the approach to risk management that will be used.



What is physical security and how does it work?

Physical security is the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to an enterprise, agency or institution. This includes protection from fire, flood, natural disasters, burglary, theft, vandalism and terrorism. While most of these are covered by insurance, physical security's prioritization of damage prevention avoids the time, money and resources lost because of these events.

Access control
Surveillance
Testing

ethical and legal issues in computer security

- Most ethical and legal issues in computer system are in the area of individual's right to privacy versus the greater good of a larger entity i.e. a company or a society. For example, tracking how employees use computers, crowd surveillance, managing customer profiles, tracking a person's travel with passport and so on. A key concept in resolving this issues is to find out, what is a person's expectation of privacy. Classically, the ethical issues in security system are classified into following 4 categories:
- **Privacy:** This deals with the right of an individual to control personal information. It is the protection of personal or sensitive information. Privacy is subjective. Different people have different ideas of what privacy is and how much privacy they will trade for safety or convenience.
- **Accuracy:** This talks about the responsibility for the authenticity, fidelity an accuracy of the information.
- **Property:** This determines who the owner of the information is and who controls access.
- **Accessibility:** This deals with the issue of the type of information, an organization has the right to collect. And in that situation, it also expects to know the measures which will safeguard against any unforeseen eventualities.
- When dealing with legal issues, we need to remember that there is hierarchy of regulatory bodies that govern the legality of information security. The hierarchy can be roughly described as follows:
- International: e.g. International Cybercrime Treaty
- Federal: e.g. FERPA, GLB, HIPAA
- State: e.g. UCITA, SB 1386 etc.
- Organization: e.g. Computer Use policy