|  |  |
| --- | --- |
| **Strategic Plan** | **Long term plan**  **Defines the organization’s security posture**  **Useful for at least 5 years. Reviewed annually**  **Helps understand security function and align it with business**  **Should include Risk Assessment** |
| Tactical Plan | Mid-term plan developed to provide more detailed goal  Usually for an year or two  More technology oriented  Eg: Project plans, acquisition plan, budget plan, hiring plan |
| Operational Plan | Short-term plan  Highly-detailed plan  Must be updated often (monthly, quarterly)  Spell-out how to accomplish various goals  Eg: resource allotment, budgetary allocation, training plans |

**Due care** -Taking reasonable care in protecting the organization. It’s a legal term – it pertains to the legal duty of the organization. Lack of due care is considered negligence

**Due Diligence**- Practicing the activities that maintain the due care effort. Pertains to best practices that a company should follow. It might not be legally liable

**Organizational policy**- org wise. **Issue specific**-focus on specific department, function. **System specific-**focus on individual systems.

Microsoft Threat categorization scheme

**S**POOFING,**T**AMPERING,**R**EPUDIATION,**I**NFORMAITON DISCLOSURE,DENIAL OF SERICE, **E**LEVATION OF PRIVILEGES

**Reduction analysis**

Involves decomposing the application, system or environment

Purpose of this process is to get a greater understanding on the purpose of the product and its interactions with external entities

Each element should be evaluated to understand inputs, processing, security, data management, storage and output

**5 key concepts to be aware of**

**Trust Boundaries – location where the level of trust changes; Data flow paths – movement of data between locations; Input points – locations where external input is received; Privilege Operations – Activity that requires greater privileges; Security stance and approach – Declaration of the security policy, security foundation and security assumptions…**