**Module 5 Risk Management**

**5.7 Controls**

**Security Controls**

* Technical
* Administrative
* Physical
* Deterrent
* Preventive
* Detective
* Corrective
* Compensating

**Controls**

* Defence/countermeasure put in place to manage risk
* Cybrary – Policies, strategies, technologies, configuration settings etc. established in collaboration with various departments of organisation to mitigate known risks
* ISACA – means of managing risk, including policies/procedures/guidelines/practices or organisational structures which can be of administrative/technical/management/legal nature

**Technical/Logical**

* Implemented through technology
* May be deterrent/preventive/detective/compensating
* Eg. Patching, firewalls, IDS/IPS, access controls

**Administrative/Management**

* Documents, policies, procedures & guidelines

1. Acceptable Use Policy
2. Incident Response Plan

* People/personnel

1. Security operations centre
2. Guards
3. Surveillance
4. Security awareness training

**Physical/Operational**

* Reduce risk of harm coming to physical property/information/computer systems/other assets
* Eg. Hardened facilities, locks, badges

**Deterrent Controls**

* Intended to discourage individuals from intentionally violating security policies/procedures/technologies
* Highly visible
* Prevent offenses/abuses by influencing choices

**Preventive Controls**

* Stop unwanted event (breach, fraud, outage, errors etc.)
* Proactive measures
* Examples

1. Access, authentication, authorisation, verification
2. Separation of duties
3. Technical standards
4. Network security – firewalls, IPS
5. Internet filtering

**Detective Controls**

* Warning of anomalies/violations
* Automated or manual
* Reactive
* Eg. Cameras, motion sensors, IDS/SIEM, audits

**Corrective Controls**

* Measures to lessen harmful effects/restore system being impacted
* Mostly reactive measures
* Eg. Patching/upgrades, hardening (physical & logical), process improvements

**Compensating Controls**

* Alternate controls intended to reduce risk of existing/potential control weakness
* Mechanism (process, technology etc.) that satisfies required security measure
* PCI DSS (Payment Card Industry Data Security Standard)

1. Meet intent & rigor of original stated requirement
2. Provide similar level of defence as original requirement
3. Be “above & beyond” other requirements
4. Be commensurate with additional risk imposed by not adhering to requirements