

Security Controls



Kevin Henry

CISM CISSP CCSP

kevin@kmhenrymanagement.com



Security Principles for the CCSM Certification

Agenda:

**Information Security Concepts
and Governance**

Risk Management

Security Controls

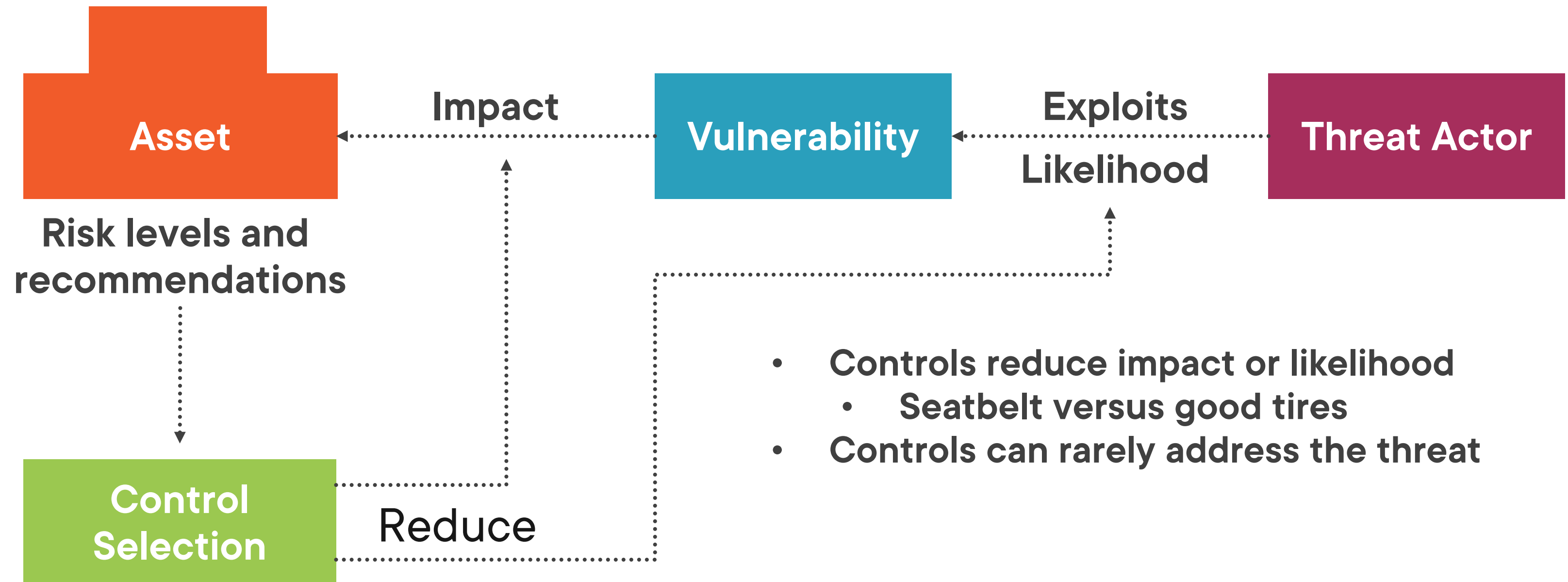
(ISC)² Code of Ethics



Risk and Control



Risk Treatment



Types of Controls

**Administrative /
Managerial**

**Technical /
Logical**

**Physical /
Environmental**



Security Controls

Proactive

Safeguards

- Directive
- Deterrent
- Preventive

Reactive

Countermeasures

- Detective
- Corrective
- Recovery

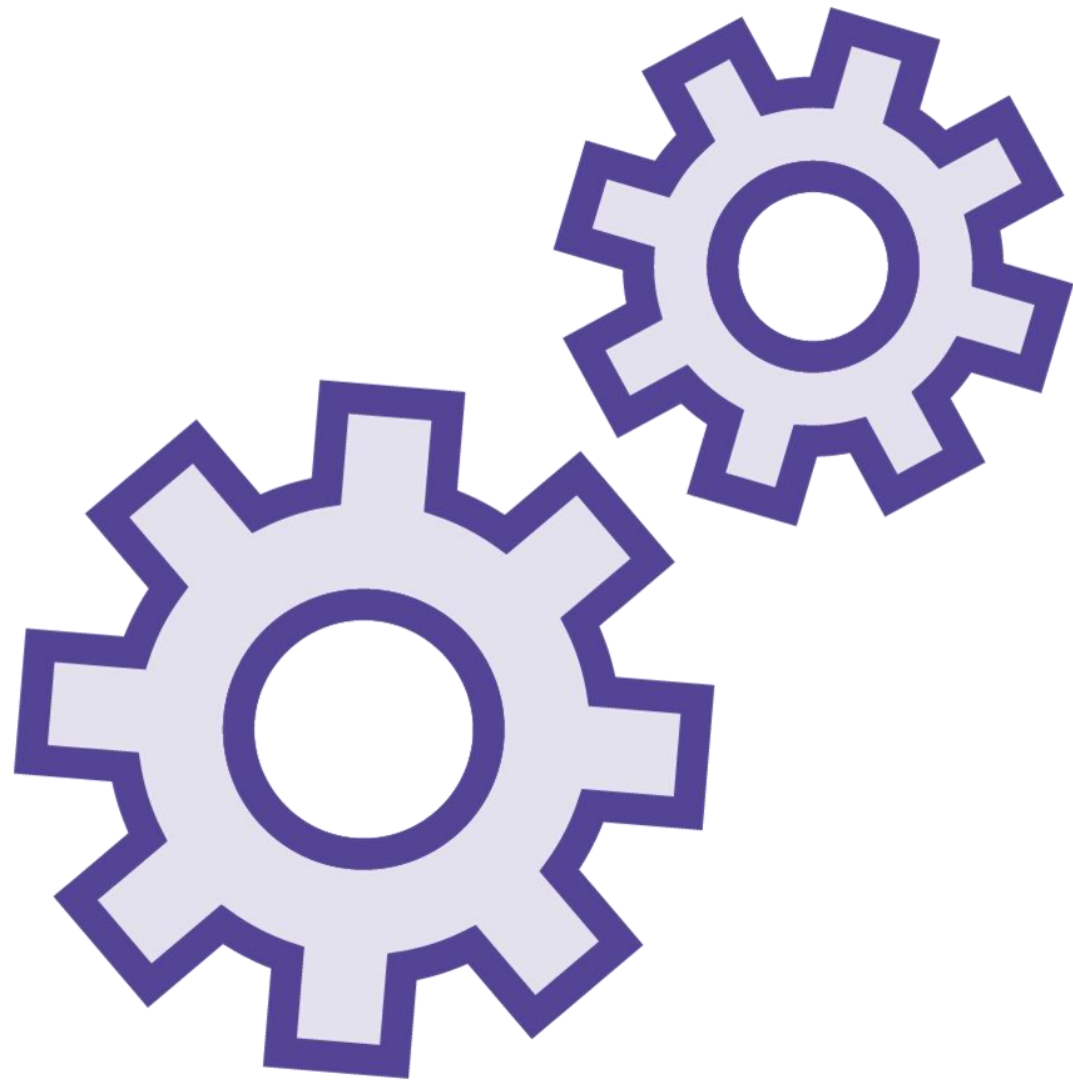


Controls

Type	Managerial	Technical	Physical
Directive	Policy	Warning banner	‘Do not Enter’ sign
Deterrent	Disciplinary action	Notification of monitoring	‘Beware of Dog’ sign
Preventive	Separation of duties	Password	Fence
Detective	Audit	Logs, IDS	Smoke detector
Corrective	Employee suspension	System isolation	Fire extinguisher, mantrap
Recovery	Awareness sessions	Rebuild from backups	Rebuild



Control Selection



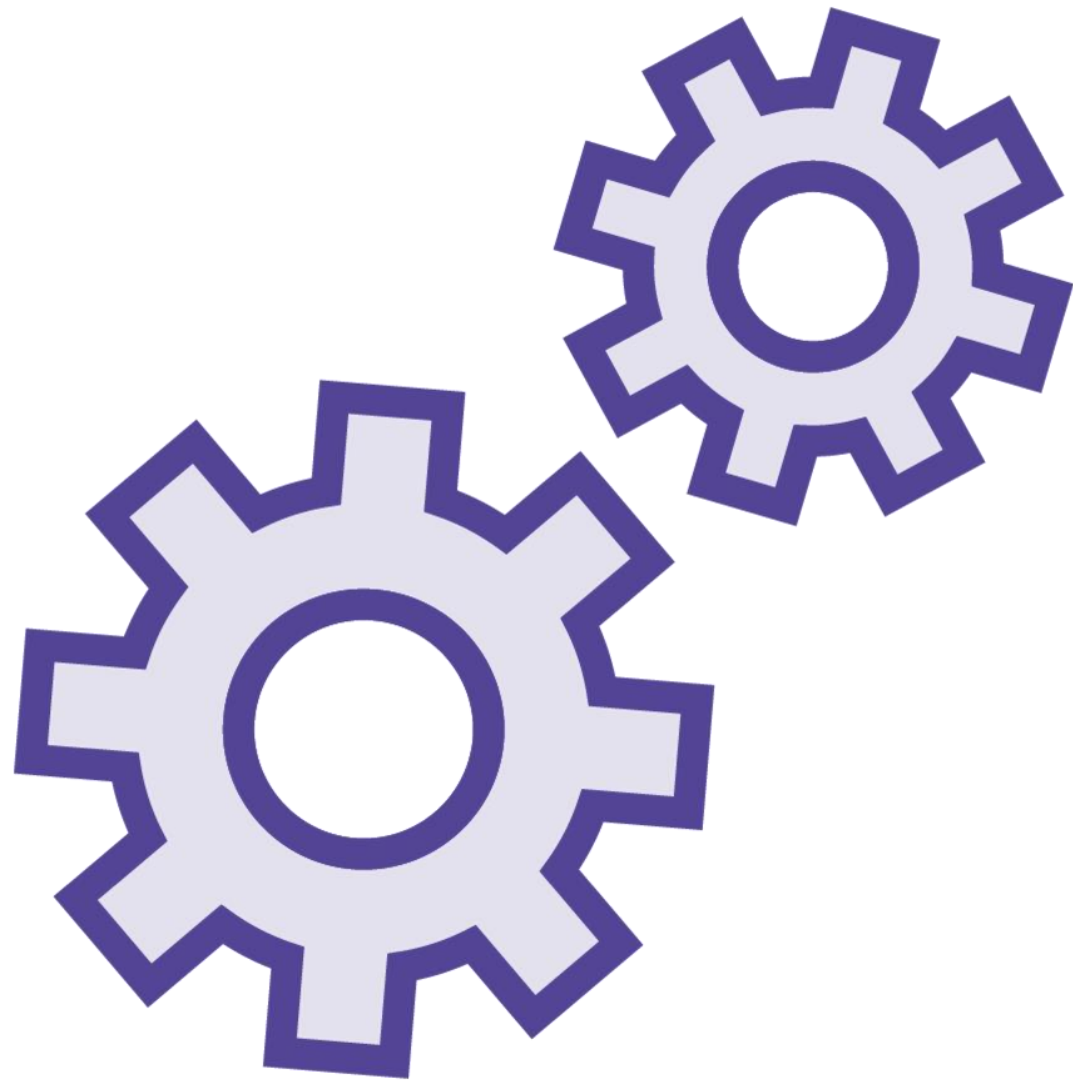
Identify recommended or required controls:

- NIST SP 800-53
- PCI-DSS

Determine which controls are available

- Timeliness
- New controls or enhanced controls
- May require more than one control

Control Cost and Documentation



Calculate the cost of the control versus the benefit that the control may provide

- Cost/benefit analysis (CBA)

Update the risk register



Key Points Review



Risk justifies controls

Controls are selected based on:

- Risk Appetite
- Availability of controls
- Cost/benefit analysis (CBA)

