

Security Operations and Administration



Kevin Henry

CISM CISSP CCSP

kevin@kmhenrymanagement.com



Security Operations for CCSM Certification

Agenda:

Data Security

**Security Operations and
Administration**

Security Awareness Training

**Exam Review Tips and
Techniques**



Security Health



Governance

- Active management commitment to the security strategy
- Monitoring
- Compliance
- Enforcement



Policies



Signed by management

Communicated

Mandate requirements

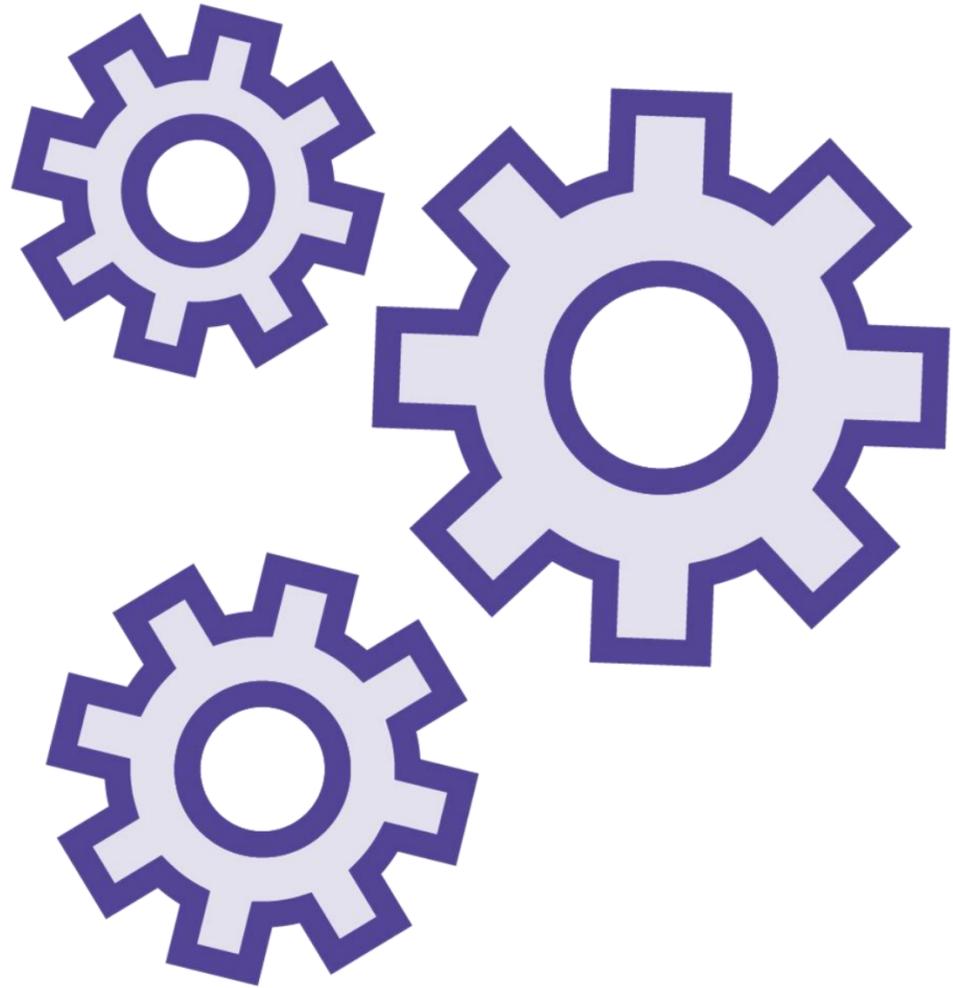
- Influence behaviors

Disciplinary action

Up-to-date



Functional Policies



Address specific technologies or areas of concern

Often implemented through procedures, standards, baselines



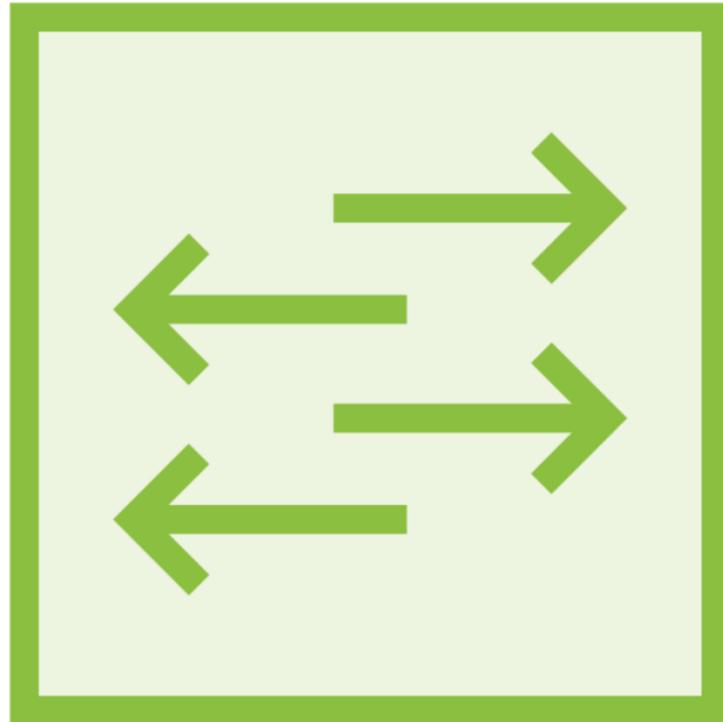
Acceptable Use Policy



Business only versus “Reasonable” use
Restrictive versus permissive approach
Piracy



Data Handling Policy



Need to know

Sharing data

Inference

Aggregation

Destruction

Clean desk

Clear screen



Password Policy



Length

Complexity

Expiry

Sharing

- Between systems
- With others



Bring Your Own Device Policy



Choose your own device (CYOD)?

Configuration

Right to audit

Sandbox – virtual machine



Privacy Policy



Laws and Regulations

Need to know

Obfuscation of data

Screen filters

Investigations



Configuration Management



Baseline Configuration



Required standard configuration

- Hardware
- Software
- Security tools
 - Firewall
 - Anti-malware

Auditable



Changes to Configurations

Fixes and upgrades to:

- Software
- Network configuration
- Projects
- Hardware

Patches



Change Control

Documented

Tested

Authorized



Change Planning



Communicate change

Image

Rollback



Key Points Review



Configuration management ensures that all systems are deployed (configured) in an approved secure manner

Change is a time of risk – so controlling changes to the configuration baseline is important

