

Domain Summary



Kevin Henry

CISM CISSP CCSP

kevin@kmhenrymanagement.com

Security Principles for the CCSM Certification

**Information Security Concepts
and Governance**

Risk Management

Security Controls

(ISC)² Code of Ethics



Key Points

Security is a part of the business process and should support business operations and strategy

Organizational governance requires management to 'own' security and be accountable for it

Key Points – CIA Triad



Key terms used to define information security include:

- Confidentiality
- Integrity
- Availability

Key Points – Risk Management



Risk must be managed and ‘owned’

- Risk identification
- Risk treatment/response
- Risk monitoring

Risk acceptance levels are determined by the risk owner – senior management

The goal of risk management is to ensure that all risk (residual) is within risk acceptance levels

Key Points - Controls



Controls are justified by and mitigate risk

Safeguards and countermeasures

- Administrative/managerial
- Technical/logical
- Physical/environmental

Code of Ethics



Mandated for all certification holders

Enforced by the Board of Directors

Next Steps



Review and understand each topic area – not just memorization

Do the sample questions in the Study Guide

Proceed to the next domain – Business Continuity, Disaster Recovery, and Incident Response