University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001/27002

CS 4950/5950
Homeland Security & Cybersecurity

Lesson 23
ISO 27001/27002

Rick White, Ph.D.
University of Colorado, Colorado Springs

1
Esc

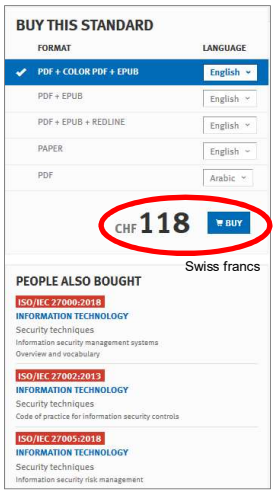
1

University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001/27002

- ISO 27001 Information Security Management System
  - Management Framework
- ISO 27002 Code of Practice for Information Security Controls
  - Control Practices



2
Esc

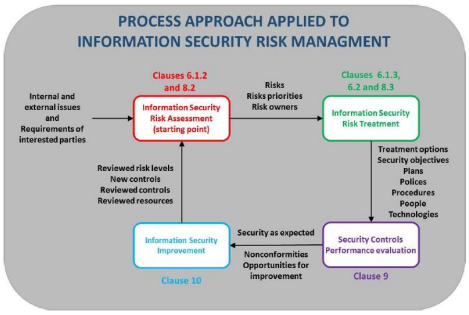
2

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Process

- Step 1: Risk Assessment
- Step 2: Risk Treatment
- Step 3: Performance Evaluation
- Step 4: Corrective Action



3
Esc

3

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Organization

- Leadership Commitment
- Policy Support
- Appropriate Authority

The Gist of It…

It takes the entire village to make cybersecurity work… and only one village idiot to break it.

4
Esc

4

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Understanding

- Inputs
- Processes
- Outputs

Sun Tzu
The Art of War

If you know the enemy and know yourself, you need not fear the result of a hundred battles.

If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.

If you know neither the enemy nor yourself, you will succumb in every battle.

5
Esc

5

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Step 1: Risk Assessment

a) Define Risk Assessment Method
b) Identify Risks & Risk Owners
   – In this context, "Risks" are things that could go wrong
c) Assess Probability & Consequence of Risks
d) Calculate Risk Magnitude
   – M(R) = P(R) x C(R)
e) Establish Risk Threshold
   – If M(R) > n then R = priority
f) Output = Risk List = Prioritized List of Risks and Who Owns Them

Risk Assessment Method

ISO 27001:2013, the current version, does not define a risk methodology. The previous version, ISO 27001:2005, prescribed a specific risk methodology. The change was made to make the standard more flexible (i.e., you could still do something else and be "compliant").

6
Esc

6

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Step 2: Risk Treatment

a) For each risk on the Risk List, determine course of action:
   - Apply Security Control (114)
   - Transfer Risk (e.g. insurance)
   - Avoid Risk (e.g., stop activity)
   - Accept Risk (i.e., do nothing)

b) Write Statement of Applicability
   - Justifies Treatment Selection

c) Write Risk Treatment Plan
   - Treatment Plan of Action

Security Controls

Annex A to ISO 27001 has a list of 114 Security Controls that can be applied to mitigate an identified risk. ***ISO 27002 has detailed guidance of the application of Security Controls listed in ISO 27001 Annex A.***

Statement of Applicability

Why justify selected treatments? Justification helps make the business case to management "why" they should invest in recommended treatment actions.

7 Esc

7

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Control Implementation

Somewhere between Step 2 and Step 3, security controls and other measures are implemented according to the Risk Treatment Plan.

Big Difference
ISO 27001, NIST RMF, and ES-C2M2

Although all three models evaluate risk, unlike NIST RMF and ES-C2M2, ISO 27001 doesn't require a cost-benefit-analysis on proposed Security Controls.

8 Esc

8

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Step 3: Performance Evaluation

a) Develop/Update ISMS Performance Evaluation Plan
   - Measures of Compliance
   - Measures of Actions
   - Measures of Conformance
b) Conduct Periodic Audits
   - Independent Auditors
   - Identify Deficiencies

Performance Measures

Compliance	*Meeting Standards?*
Actions	*Effective Responses?*
Conformance	*Achieving Objectives?*

9

Esc

9

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Step 4: Corrective Action

a) Review Audit with Management
b) Document Decisions
c) Initiate Next Cycle of ISO 27001

Management Review

Management review is important for gaining leadership support, and smoothing way ahead for next cycle of ISO 27001.

10

Esc

10

University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Conclusion

Questions?

11

Esc

11