
Lessons Learned in IT:
The Role of DHS Essential Body of
Knowledge (EBK) and ICS

Wm. Arthur Conklin, PhD

Agenda

Motivation

Introduction to EBK

Key Terms and Concepts

Competency Areas

Security Roles

Functional Event Types

Examples

How to use

Conclusions

IT Security is a complex, rapidly changing field

Training of personnel is complex

Government has battled this for years

» DoD – DHS working group

DHS releases EBK

Source of Data

- » 53 CWF from DoD
- » ISO standards
- » NIST standards
- » Industry Certifications

Parts of the EBK

- » Key Terms
- » Competencies
- » Roles
- » Functional Event Types
- » Functional Competencies

Competency Areas

1. Data Security
2. Digital Forensics
3. Enterprise Continuity
4. Incident Management
5. IT Security Training and Awareness
6. IT Systems Operations and Maintenance
7. Network and Telecommunications Security
8. Personnel Security
9. Physical and Environmental Security
10. Procurement
11. Regulatory and Standards Compliance
12. Security Risk Management
13. Strategic Security Management
14. System and Application Security

3 Types

- » Executive
- » Functional
- » Corollary

10 Roles

- » Chief Information Officer
- » Information Security Officer
- » IT Security Compliance Officer
- » Digital Forensics Professional
- » IT Security Engineer
- » IT Security Operations and Maintenance Professional
- » IT Security Professional
- » Physical Security Professional
- » Privacy Professional
- » Procurement Professional

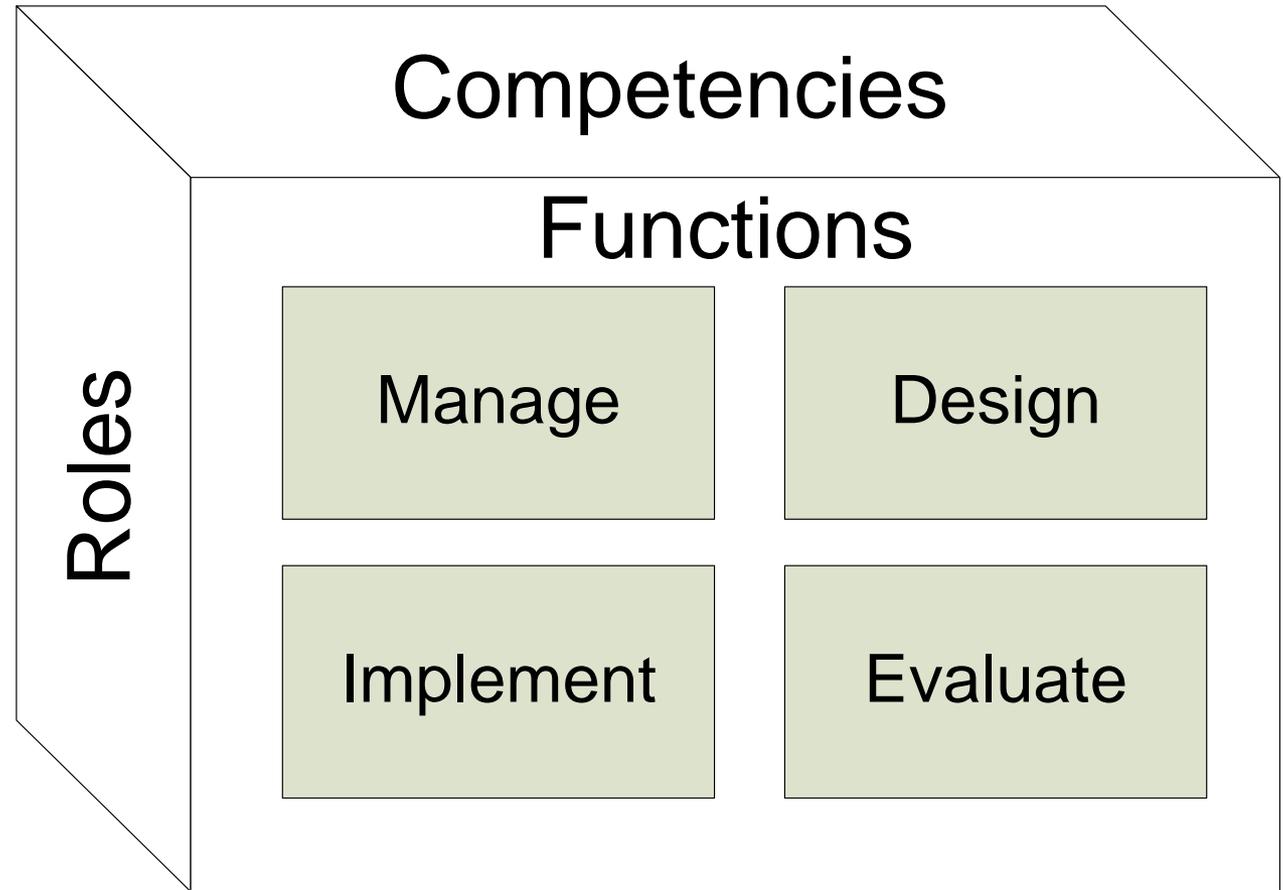
Functional Event Types

Manage

Develop

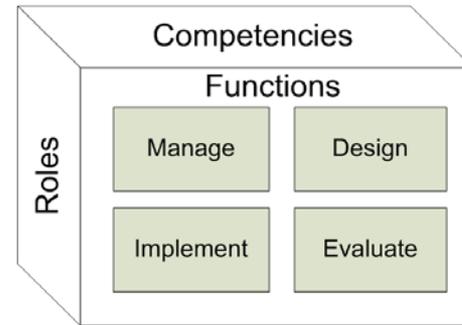
Implement

Evaluate



Enterprise Continuity competency

CIO role



Manage function sample items

- Define the enterprise continuity of operations organizational structure and staffing model
- Define emergency delegations of authority and orders of succession for key positions

Map jobs to Roles

Examine Competencies by role

Customize Functional Requirements

Document results

So Where are ICS Categories?

Competencies

1. Data Security
2. Digital Forensics
3. Enterprise Continuity
4. Incident Management
5. IT Security Training and Awareness
6. IT Systems Operations and Maintenance
7. Network and Telecommunications Security
8. Personnel Security
9. Physical and Environmental Security
10. Procurement
11. Regulatory and Standards Compliance
12. Security Risk Management
13. Strategic Security Management
14. System and Application Security

Roles

3 Types

- Executive
- Functional
- Corollary

10 Roles

- Chief Information Officer
- Information Security Officer
- IT Security Compliance Officer
- Digital Forensics Professional
- IT Security Engineer
- IT Security Operations and Maintenance Professional
- IT Security Professional
- Physical Security Professional
- Privacy Professional
- Procurement Professional

Problems

Majority of vulnerabilities are in “ordinary IT aspects”

- Patches
- Antivirus/Antispyware

ICS computers can be “upset” by standard security testing

By whom and how managed

Controls

Training

EBK forms basis for IT Security Training

How to align training with ICS and Security

- Train IT Security – Control Requirements
- Control Personnel – IT Security

EBK can be modified to allow management

EBK is a proven methodology

Modifications to EBK

SMEs

- ICS
- Security

Conclusion

Training requirement determination is challenging

Framework is flexible

Framework is extensible

Organizes complex subject

Can be expanded to include ICS

My next step

Sit down and color with the other kids



Questions?
Ask this guy:

Wm. Arthur Conklin, PhD

Assistant Professor

Director

Center for Information Security Research and Education

College of Technology

University of Houston

waconklin@uh.edu

<http://tech.uh.edu/faculty/conklin>