Securing a Control System: Experiences from ISO 27001 Implementation

Vasu Vuppala, Ph.D., John Vincent, Ph.D., Jay Kusler; Kelly Davidson

National Superconducting Cyclotron Laboratory, East Lansing, Michigan, USA

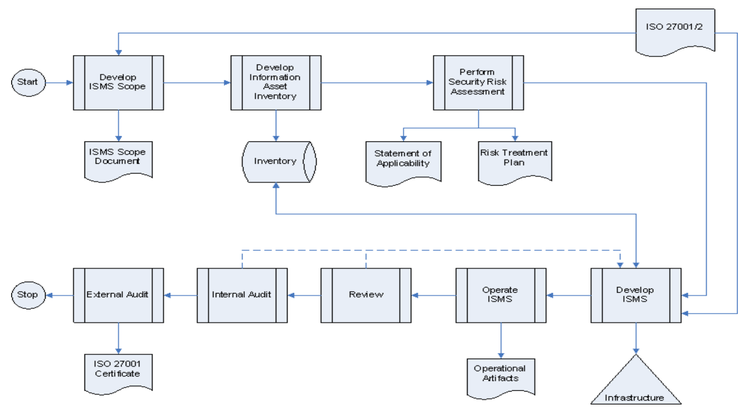
Introduction

Recent incidents have emphasized the importance of security and operational continuity for achieving the quality objectives of an organization, and the safety of its personnel and machines. However, security and disaster recovery are either completely ignored or given a low priority during the design and development of an accelerator control system, the underlying technologies, and the overlaid applications. This leads to an operational facility that is easy to breach, and difficult to recover. Retrofitting security into the control system becomes much more difficult during operations.

Objective

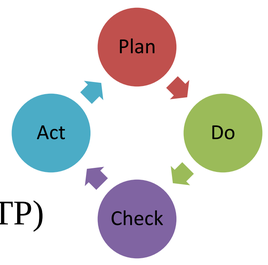
The Electronics Department at NSCL wanted to address security in a holistic manner, and decided to implement ISO/IEC 27001 Information Security standard. The ISO/IEC 27001 standard and the related code of practice (ISO 27002) cover a broad set of topics such as risk assessment, asset management, human resources, physical security, communication and operations, , application development and maintenance, access control, disaster recovery, security incident management, and legal and regulatory compliance.

Roadmap



Lifecycle

- Plan
  - Define Scope and ISMS Policy
  - Develop Approach to Identify, Evaluate, and Treat Risks
  - Identify and Analyze Risks. Evaluate Risk Treatment Options
  - Select Controls to Treat Risks
- Check
  - Monitor and Review Argus. Conduct Internal Audits
  - Measure Argus' Effectiveness
  - Review Risk Assessment
- Do
  - Develop Risk Treatment Plan (RTP)
  - Implement RTP
  - Measure Effectiveness of Controls
  - Manage Information Security Incidents
  - Implement Training and Awareness Programs
- Act
  - Identify Improvements
  - Corrective and Preventive Actions



Controls

- Asset Management
- HR Security
- Physical Security
- Communication and Operations Management
- Access Control
- Information Systems Development
- Information Security Incident Management
- Business Continuity Management.
- Compliance

Asset Classification

#	Class	Description
1	Class I	The information is very sensitive, and must be released only to an authorized group of people. Example: HR data in IFS
2	Class II	The information related to and on the Control Network. Example: PV Data, IOC configuration
3	Class III	The information that is accessible only to the employees, students, and contractors working in the Electronics Department. Example: Information on Intra Enterprise or the files in the I: drive
4	Class IV	Information related to user experiments including the results of the experiments.
5	Class V	The information is not sensitive and can be released to public at large. Example: Pages on NSCL website

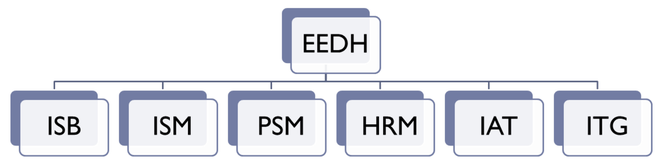
Risk Assessment

Impact	Value
No Impact	0
Low	1
Medium	2
High	3

Impact Area (IA)	IA Priority	Impact Value	Score
Safety and Health	5	Low (1)	5
Reputation	4	Med (2)	8
Financial	3	High (3)	9
Legal	2	None (0)	0
Productivity	1	Low (1)	1
Relative Risk Score			23

Probability	Relative Risk Score			
	60+	40 to 59	20 to 39	0 to 19
High	Level I	Level I	Level II	Level III
Medium	Level I	Level II	Level II	Level IV
Low	Level II	Level II	Level III	Level IV

Security Organization

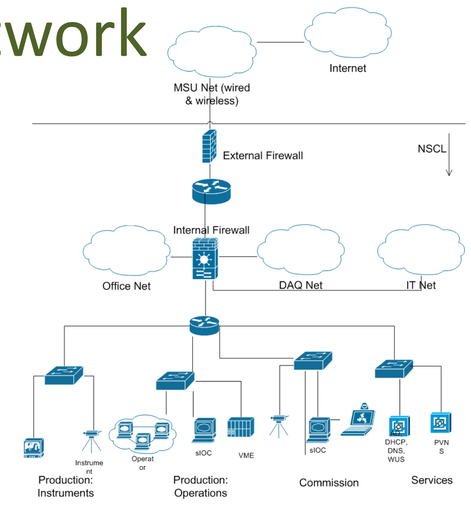


- EE Department Head (EEDH), Information Security Board (ISB)
- Information Security Manager (ISM), Physical Security Manager (PSM)
- Human Resource Security Manager (HRSM)
- Internal Audit Team (IAT), IT Management Group (ITG)

Risk Profile & Treatment

				Threat Scenario							Impact Value								Treatment				
#	Risk ID	Threat Scenario	CIA ID	Actor	Means	Motive	OC	SR	P	Consequences	QO	REP	PRD	SNH	FIN	LGL	CPS	Score	Avoid	Reduce	Transfer	Accept	Owner
1	RSK-PLC2	Production Safety PLC's logic can be modified by connecting to it over the network	CIA-PSW	Disgruntled Employee	PLC Software	Malicious	M,T	I	M	Danger to human health/life	2	3	2	3	3	3	0	58	Prevent modifications to PLCs through physical keys. Check PLC types for security provisions. Devise process to manage keys.	See SoA	No	Accept Residual Risk	Kelly, Vasu
2	RSK-PLC1	Production Control System PLC's logic can be modified by connecting to it over the network	CIA-PSW	Disgruntled Employee	PLC Software Tools	Malicious	M,T	I	M	Equipment damage	3	3	3	1	3	1	0	50	Same as RSK-PLC2	See SoA	No	Accept Residual Risk	Kelly, Vasu

Network

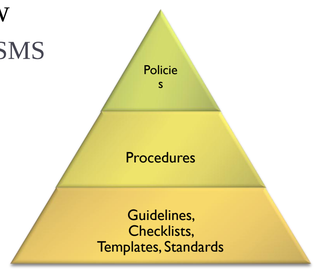


Access Control Matrix

		Information Class				
		Class I	Class II	Class III	Class IV	Class V
Access Medium	Control Network	Not Allowed	No Controls for PVs and Embedded Controllers. Authorization for other data.	Authorization, Encryption	Authorization, Encryption	No controls for read. Authorization, encryption for write.
	DAQ Network	Not Allowed	No controls for read. Authorization for write.	Authorization, Encryption	Authorization, Encryption	No controls for read. Authorization, encryption for write.
	Office Network	Authorization, Encryption	No controls for read. Authorization for write.	Authorization, Encryption	Authorization	No controls for read. Authorization, encryption for write.
	MSU Wired Network	Not Allowed	Not Allowed	Not Allowed	Authorization, Encryption	No controls for read. Writes not allowed.
	MSU Wireless Network	Not Allowed	Not Allowed	Not Allowed	Authorization, Encryption	No controls for read. Writes not allowed.
	Internet	Not Allowed	Not Allowed	Not Allowed	Authorization, Encryption	No controls for read. Writes not allowed.
	Physical Access	Authoization and swipe card	Authorization, Swipe Card, and Key	Authorization and Swipe Card	Authorization and Swipe Card	No controls for read. Writes not allowed.

Documentation

- Argus Handbook: Informal Overview
  - Argus ISMS Policy: Formal Policy for ISMS
    - Argus ISMS Procedure: PDCA Steps
  - Argus Documentation Policy
    - Argus Document Procedure
  - Management Responsibilities
  - Internal Audits Procedure
  - Management Review Policy
  - Argus Corrective and Preventive Action Policy
  - Argus Controls
    - Policy, Procedures, Guidelines etc from ISO/IEC 27002



Lessons Learnt

- Start Small. Implement. Expand.
- Not Necessary to Include Whole of IT
- Leverage Existing Management Systems: ISO 9001, 18001, 14001 etc
- Reserve Resources, If Possible
- Management Support is Crucial
- Needs Support From Every Unit in the Organization

Challenges

- Research and Education Environment
- Organizational, Infrastructure Changes
- Implementing Secure Software Development Practices
- Interest Level: Non-technical and Mundane Work
- Technical
  - Control Net: No Encryption, Authentication, Authorization
  - Cabling, Password Aging, Employee Agreements

Conclusion

- Completed: RA, Documentation, Registrar Selection
- Expected Date of Certification: Jan 2012
- Effort: ~1000 Person Hours Planned. ~800 completed
- Provided Insights To Risks and Threats
- Improved Network, Database, Application Design

This work was supported in part by the National Science Foundation under the Cooperative Agreement PHY-06-06007.