National Superconducting Cyclotron Laboratory

MICHIGAN STATE UNIVERSITY

Securing a Control System:
Experiences from ISO 27001 Implementation

Vasu Vuppala, Ph.D., PMP
John Vincent, Ph.D.
Jay Kusler
Kelly Davidson
{vuppala,vincent,kusler,davidson}@nscl.msu.edu

National Superconducting Cyclotron Laboratory,
East Lansing, Michigan, USA.

Overview

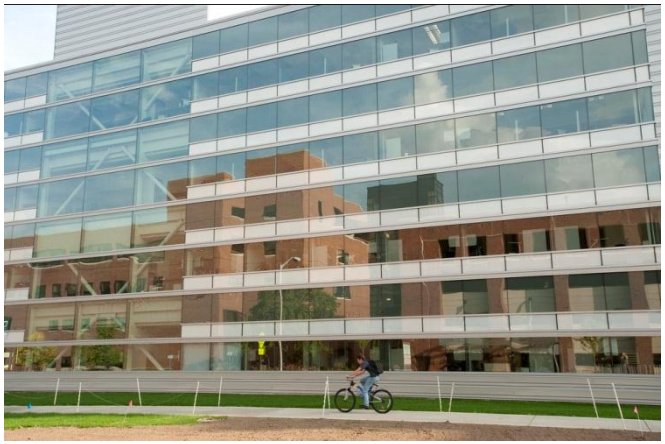
- Background
- ISO/IEC 27000
- Argus the ISMS
  - Risk Assessment
  - Controls
  - Lifecycle
- Retrospection
  - Project Statistics, Challenges
  - Lessons Learnt
  - FRIB Data Security
- Conclusion

NSCL

The Problem

Background: NSCL

- Rare Isotope Research
- Two Superconducting Cyclotrons
- Located on Campus of Michigan State University, USA
- About 400 Employees
- Building the Facility for Rare Isotope Beam (FRIB)
- Electronics Department
  - RF, Power Supplies, Control Instrumentation, Controls Software
  - Approx 40 Employees



Background: The Initial Problem

- Restrict Traffic to Control Network
- Reduce Inadvertent Disruptions to Experiments
- Group Based Access Control to EPICS Channels
  - Groups of Devices
  - Groups of Users
- Ability to Reserve/Release Devices (Their Channels)
- Solutions
  - Updating IOC database, and reload
  - Modify Channel Access
- More Problems: IOC Security, Embedded Controllers, PLCs, Network, Servers, License Keys, Physical Access, People ….

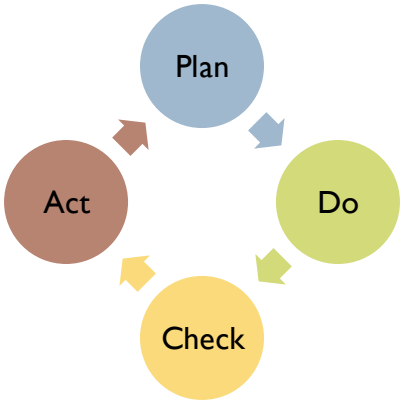
ISO/IEC 27000

ISO/IEC 27000 Series Standards

- 27000 – Overview
- 27001 – Specification
- 27002 – Code of Practice (Controls)
- 27003 – Implementation Guidance
- 27004 – Information Security Management Measurement
- 27005 – Information Security Risk Management
- 27006 – Certification/Registration Process

ISO/IEC 27001

- The Specification
- Process Approach: Plan-Do-Check-Act (PDCA) Model
- Defines ISMS Requirements
  - Establish, Implement and Operate, Monitor and Review, Maintain and Improve
- Documentation Requirements
- Management Responsibilities
  - Commitment, Resources, Training, Awareness
- Internal Audits
- Management Review
- ISMS Improvement
  - Corrective and Preventive Actions



ISO/IEC 27002

- A Code of Practice: Annex to 27001
- Security Clauses (11)
  - Main Security Categories (39)
    - Security Objective
    - Security Controls
- Security Clauses
  - Security Policy
  - Information Security Organization
  - Asset Management
  - HR Security
  - Physical Security
  - Communication and Operations Management
  - Access Control
  - Information Systems
  - Information Security Incident Management
  - Business Continuity Management
  - Compliance

NSCL

Argus The ISMS

Argus The ISMS

- Information: Data that is important to an organization.
- Information Security - Preservation of the Following for Information:
  - Confidentiality: Not Disclosed to Unauthorized Entities
  - Integrity: Accuracy and Completeness
  - Availability: Accessible and usable upon demand

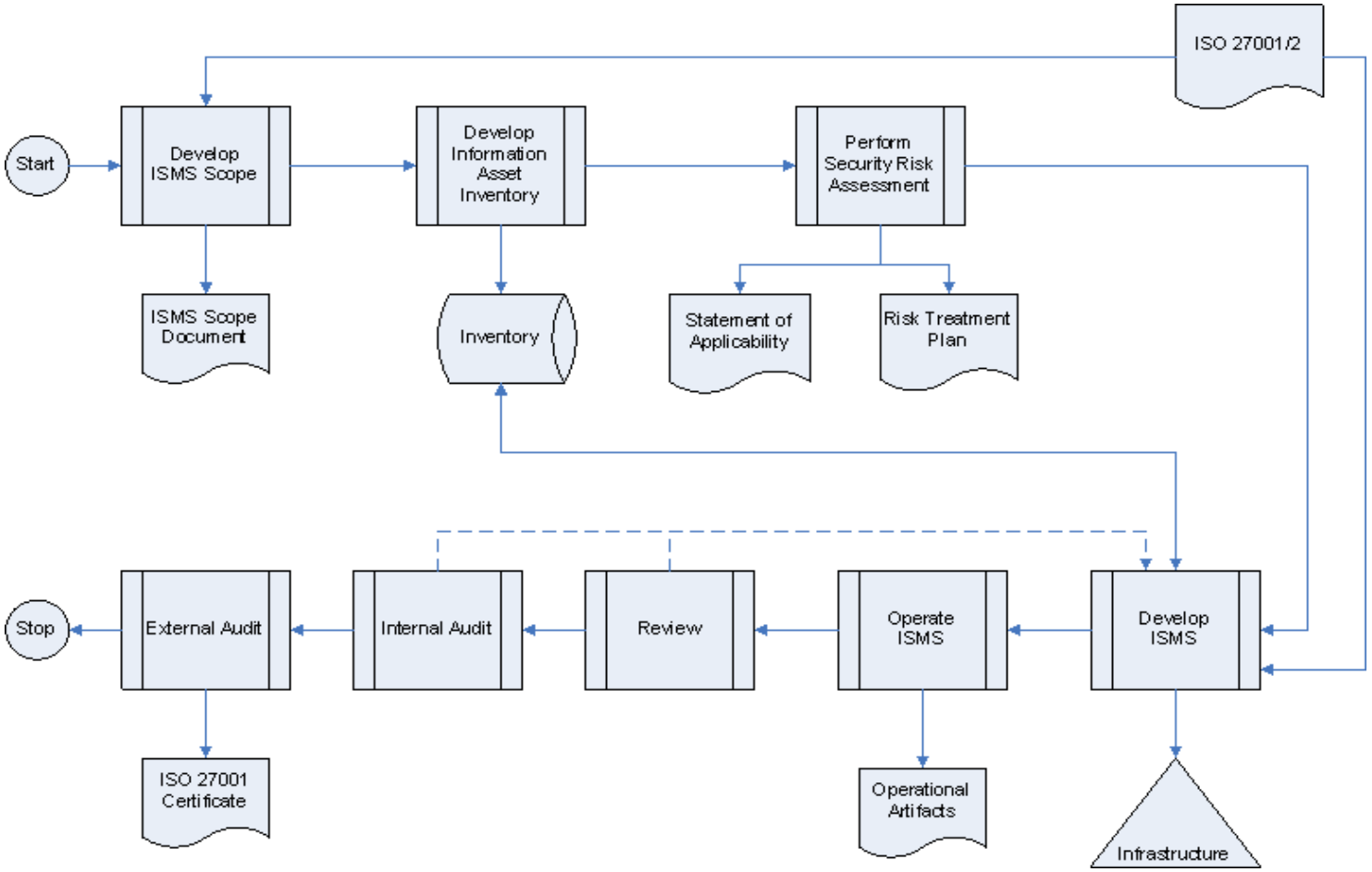
- Management System: Framework of policies, procedures, guidelines and associated resources to achieve the objectives of the organization
- Information Security Management System (ISMS): A management system to establish implement, operate, monitor review, maintain, and improve information security.

Information Security

- Requirement Sources
  - Assessing Risks to the Organization
  - Legal, Regulatory, Contractual Compliance
  - Organization's objectives for Information Processing
- Protection of information from threats for business continuity, minimize risk
- Information Security is Achieved by Implementing a Set of *Controls*
- What are *Controls*?
  - Policy, Procedure, Organization Structure, Software/Hardware Functions
  - Means of Managing Risk

NSCL

Argus The ISMS: Roadmap



Argus: Risk Assessment

Information Assets, Containers, Owners

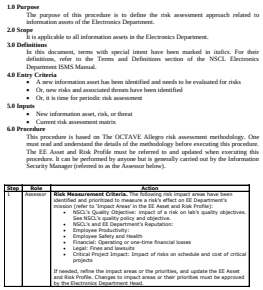
- Information Assets (IA): Information That is of Value to the Organization
  - Examples: Controls Software Source, Channel Data, IOC Configuration, HR Database etc
- IA Containers: Where Information Assets Reside/Stored
  - Technology: File Server, Software, Database etc
  - Physical: Folder, Paper, Printed Manual, etc
  - Human: Intellectual Property, Ideas, Special Processes
- Information Asset Owners, Custodians

NSCL

Risk Assessment Method

Based on OCTAVE Allegro

1. Establish Risk Measurement Criteria: Identify and Prioritize Impact Areas:
   - Employee Safety & Health, Quality Objective, Reputation, Productivity, Financial, Legal
2. Identify Information Assets
3. Identify Information Asset Containers: Technical, Physical, Human
4. Identify Areas of Concern: Conditions that can affect IA
5. Identify Threat Scenarios: Actors, Means, Motives, Outcomes
6. Evaluate Impact of Each Threat
7. Identify Risks: Threat + Impact
8. Analyze Risks



1.0 Purpose

The purpose of this procedure is to define the risk assessment approach related to information assets of the Electronics Department.

2.0 Scope

It is applicable to all information assets in the Electronics Department.

3.0 Definitions

In this document, terms with special intent have been marked in *italics*. For their definitions, refer to the Terms and Definitions section of the NSCL Electronics Department ISMS Manual.

4.0 Entry Criteria

- A new information asset has been identified and needs to be evaluated for risks
- Or, new risks and associated threats have been identified
- Or, it is time for periodic risk assessment

5.0 Inputs

- New information asset, risk, or threat
- Current risk assessment matrix

6.0 Procedure

This procedure is based on The OCTAVE Allegro risk assessment methodology. One must read and understand the details of the methodology before executing this procedure. The EE Asset and Risk Profile must be referred to and updated when executing this procedure. It can be performed by anyone but is generally carried out by the Information Security Manager (referred to as the Assessor below).

Step	Role	Action
1	Assessor	**Risk Measurement Criteria.** The following risk impact areas have been identified and prioritized to measure a risk's effect on EE Department's mission (refer to 'Impact Areas' in the EE Asset and Risk Profile): • NSCL's Quality Objective: impact of a risk on lab's quality objectives, including its ability to achieve its objective. • NSCL's and EE Department's Reputation: • Employee Productivity: • Employee Safety and Health • Financial: Operating or one-time financial losses • Legal: Fines and lawsuits • Critical Project Impact: Impact of risks on schedule and cost of critical projects If needed, refine the impact areas or the priorities, and update the EE Asset and Risk Profile. Changes to impact areas or their priorities must be approved by the Electronics Department Head.

Risk Assessment Method: Example

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

Argus: Asset and Risk Profiles

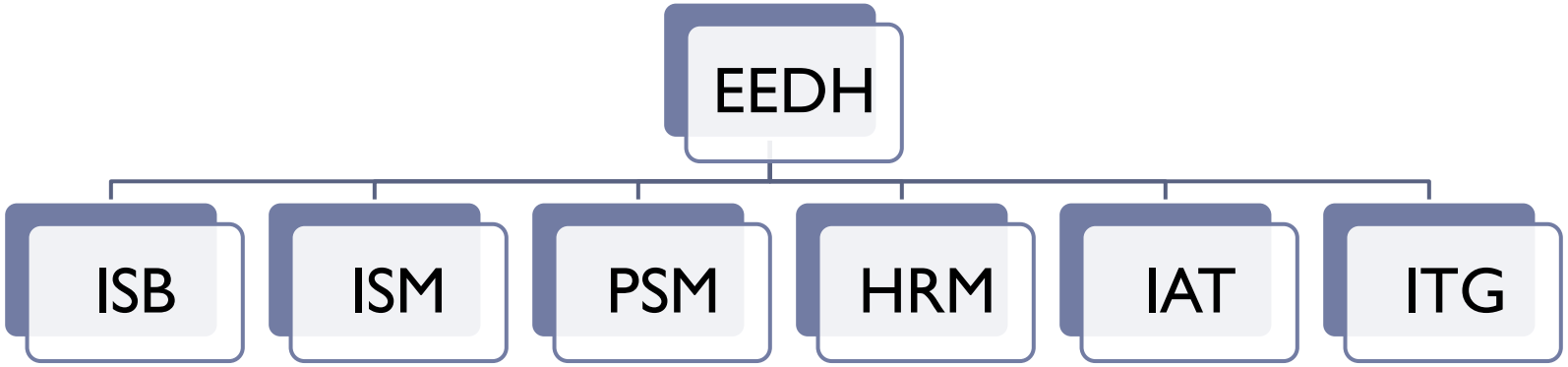
				Threat Scenario							Impact Value						
#	Risk ID	Threat Scenario	CIA ID	Actor	Means	Motive	OC	SR	P	Consequences	QO	REP	PRD	SNH	FIN	LGL	CPS
1	RSK-PLC2	Production Safety PLC's logic can be modified by connecting to it over the network	CIA-PSW	Disgruntled Employee	PLC Software	Malicious	M,T	I	M	Danger to human health/life	2	3	2	3	3	3	0
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
3	RSK-DR	Recovering from a disaster almost entirely dependent on external agency with no formal SLA	IAC-FS	EE		Disaster	T, I	A	L	Worst case: EE will not be able to recover at all. Best Case: EE will lose 2-4 weeks of work.	2	3	3	0	0	0	3
4	RSK-LIC1	Licenses, especially the physical ones, not protected, and can be stolen.	CIA-SWL1	Anyone	Physical Access	Malicious	D,I,I	A	H	Can provide access to PLC software (see RSK-PLC1 and RSK-PLC2). Monetary loss. Prevent	1	2	3	1	1	1	2
5	RSK-SW1	Documentation for many software not available/complete	CIA-CSD	Natural Disaster,			I,T	A	H	Difficult to recover from disaster. Difficult to maintain	1	2	3	0	2	0	2
6	RSK-IT	Most IT operations are outsourced with no formal SLAs	CIA-COM, IAC-	Natural Disaster,		Accident	T,I	A	H	Interruption in work. Productivity loss. Project delays.	2	2	2	0	0	0	2
7	RSK-IP	Some employees have knowledge of SW/HW for which there is no documentation or backup personnel	CIA-IP	SWG	Attrition, Leave	Accident, Malicious	I,M,T	A	H	Difficulty in fixing operational problems. Difficult to recover.	1	2	3	0	0	0	2
8	RSK-LIC2	Licenses can get destroyed.	CIA-SWL2	Natural Disaster			T	A	L	Difficult to recover from disaster. Monetary loss.	1	2	3	0	0	0	2
9	RSK-PRJ	On-going project data can get destroyed (dependent on external agency with no SLAs)	CIA-PRJ	Hardware Defect,		Accident	I,T	A	M	Productivity loss. Project delay.	0	2	2	0	0	0	3
10	RSK-DMS	Data can be modified or deleted from DMS	CIA-DMS	EE	DB or App	Accident, Malicious	M,T,I	A	M	Difficult to troubleshoot problems, or recover from disaster	1	2	2	0	0	0	2
11	RSK-ECV	EPICS PV values can be modified during an experiment	CIA-EC	EE	Software	Accident	M	I	H	Experiment becomes invalid	3	3	1	0	0	0	0
12	RSK-PLC4	Some software (PLC, Stepper Motor Controller etc) is not under configuration control	CIA-PSW	Software Defects			I,T	A	M	Difficult to revert to older versions, and to sustain the software.	1	1	3	0	0	0	2
13	RSK-HIC	Solaris server Icarus becomes unusable	CIA-CSW	SWG	Aging	Natural	I	A	H	Will not be able to build VxWorks-based IOCs.	0	2	3	0	2	0	1
14	RSK-STI	Softools IDE is crucial for embedded controllers, and the one-man supplier may go out of business	CIA-CSW	External Agency			I	A	H	No support for Rabbit-based embedded controllers. May force migration to another	0	1	3	0	2	0	1
15	RSK-ECA	Embedded Controllers do not have access control	CIA-CSW	Anyone	Network	Malicious	M,T	I	M	Equipment damage. Interruption to operations.	2	2	1	0	1	0	0
16	RSK-ARC	The EE archival cron jobs are not being monitored. They may stop working.	CIA-ARC	Natural Disaster, Humar Error	Accident	Accident	I,T	A	H	If the cron jobs stop working, some of the EE files will not be backed up onto tapes or offsite.	0	3	3	0	0	0	0
17	RSK-PLC3	A PLC's logic can get modified by accident	CIA-PSW	HWG	PLC Software	Accident	T,I	I	M	In rare cases equipment damage or safety breach	1	1	1	1	1	1	0
18	RSK-ECN	No change control process for EPICS channel names	CIA-EC	SWG	IOC Change	Accident	I,T,M	I	H	Dependent clients stop working	0	3	2	0	0	0	0
19	RSK-STM	Media of some software tools (VxWorks dev tools) may get destroyed or damaged	CIA-SIS	Accident			T,M	A	L	Old tools may not be available or supported. May have to buy new versions, and port the applications.	0	1	2	0	2	0	0

Argus Controls

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

Information Security Organization

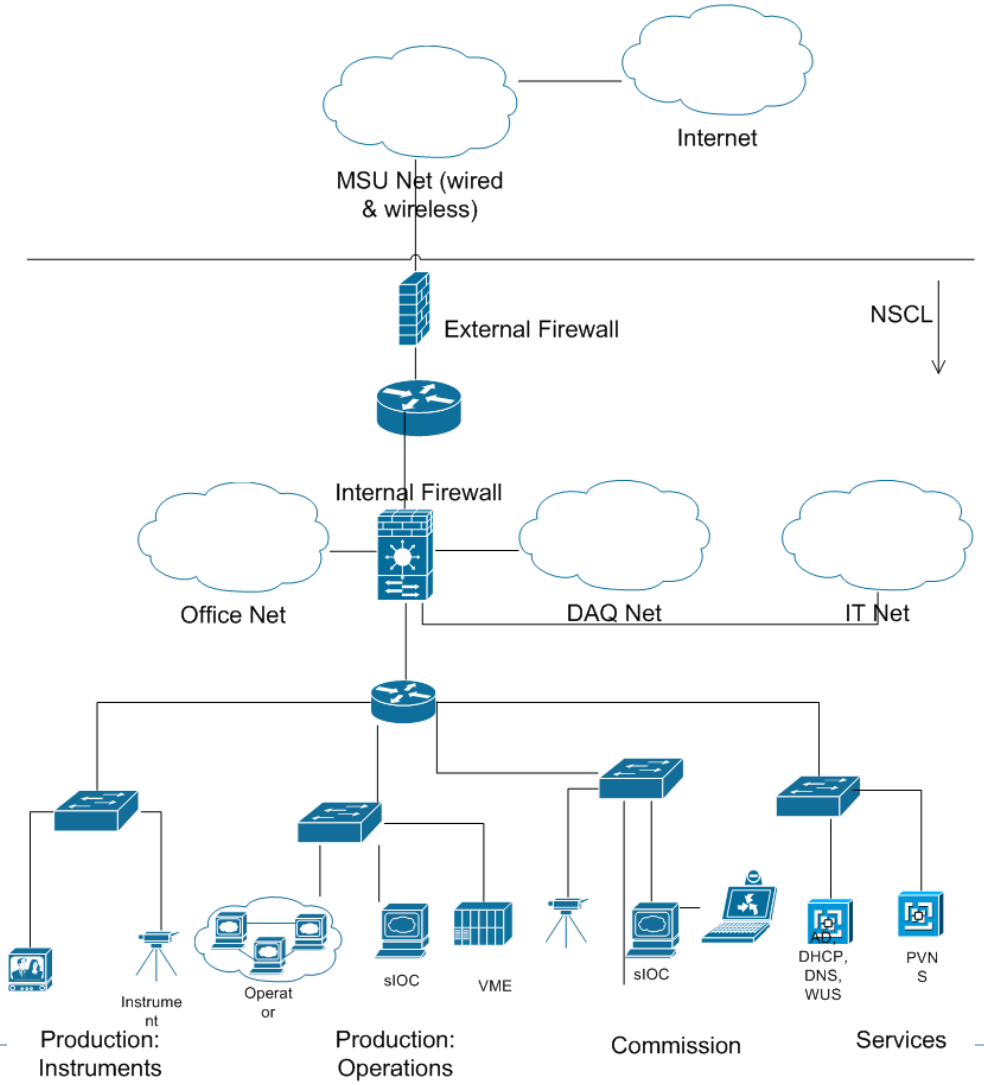


- EE Department Head (EEDH)
  - Information Security Board (ISB)
  - Information Security Manager (ISM)
  - Physical Security Manager (PSM)
  - Human Resource Security Manager (HRSM)
  - Internal Audit Team (IAT)
  - IT Management Group (ITG)

Information 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	Information related to user experiments including the results of the experiments. Example: DAQ data
4	Class IV	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
5	Class V	The information is not sensitive and can be released to public at large. Example: Pages on NSCL website

NSCL Networks



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.

Physical & HR Controls

- Physical
  - Outer Perimeter
    - Magnetic Card and PIN
    - Time Based
    - Front-desk
  - Accelerator Facility
    - Magnetic Card
- HR
  - Pre-Employment
    - Background Criminal Check
  - Post-Employment
    - Account, Entry Card Revocation
    - Assets Transfer

NSCL

Business Continuity (BC)

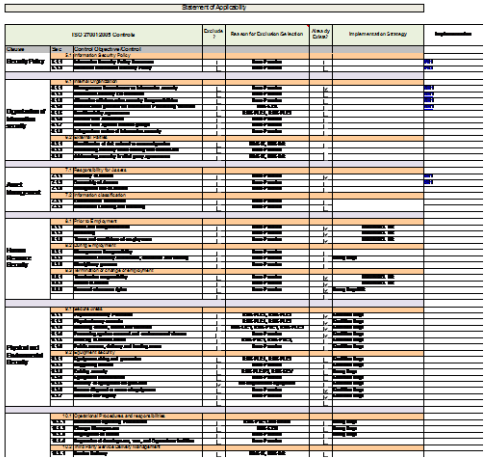
- Disaster Recovery (DR)
  - Backup Tapes Transported Offsite: Weekly
  - Offsite Live Backup (almost done)
  - Restoration Logs
  - Redundancy
- BC Procedures
  - Not Tested
  - To Be Hosted Offsite

Communication and Ops Controls

- Operating Procedures
- Change Management
- Segregation of Duties
- Separation of Development, Test, and Operational Facilities
  - Shutdowns
  - Networks to be Segregated
- Malicious and Mobile Code
- Backups
- Network Controls
- Removable Media: Handling, Disposal
- Information Exchange
- Monitoring: Access Logs, Fault Logs, Clock Sync (NTP)

Other Controls

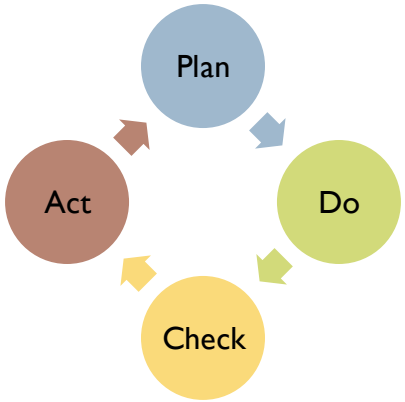
- Software Development, Maintenance, Acquisition
  - Authentication
  - No Clear Text Passwords
  - No Passwords in Code
  - Design and Code Reviews
- IS Incident Management
  - Trouble Report System
- Compliance:
  - Legal, Intellectual Property, Regulatory
  - Limited IS Requirements
- Guideline: Use Admin Account Only When Needed



Argus: Lifecycle

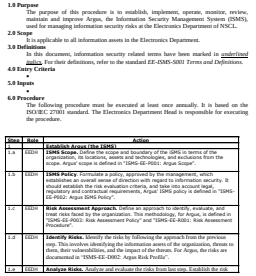
Argus: Lifecycle I

- 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: Statement of Applicability
- Do
  - Develop Risk Treatment Plan (RTP)
  - Implement RTP
  - Measure Effectiveness of Controls
  - Manage Information Security Incidents
  - Implement Training and Awareness Programs



Argus: Lifecycle II

- Check
  - Monitor and Review Argus
  - Conduct Internal Audits
  - Measure Argus' Effectiveness Based on Audits, Incidents, Feedback etc
  - Review Risk Assessment
- Act
  - Identify Improvements Based on Reviews/Audits
  - Identify and Implement Corrective and Preventive Actions



1.0 Purpose

The purpose of this procedure is to establish, implement, operate, monitor, review, maintain and improve Argus, the Information Security Management System (ISMS), used for managing information security risks at the Electronics Department of NSCL.

2.0 Scope

It is applicable to all information assets in the Electronics Department.

3.0 Definitions

In this document, information security related terms have been marked in underlined italics. For their definitions, refer to the standard *EE-ISMS-S001 Terms and Definitions*.

4.0 Entry Criteria

•

5.0 Inputs

6.0 Procedure

The following procedure must be executed at least once annually. It is based on the ISO/IEC 27001 standard. The Electronics Department Head is responsible for executing the procedure.

Step	Role	Action
1		**Establish Argus (the ISMS)**
1.1	EDH	**ISMS Scope.** Define the scope and boundary of the ISMS in terms of the organization, its locations, assets and technologies, and exclusions from the scope. Argus' scope is defined in "ISMS-EE-P001: Argus Scope".
1.2	EDH	**ISMS Policy**. Formulate a policy, approved by the management, which establishes an overall sense of direction with regard to information security. It should establish the risk evaluation criteria, and take into account legal, regulatory and contractual requirements. Argus' ISMS policy is defined in "ISMS-EE-P002: Argus ISMS Policy".
1.3	EDH	**Risk Assessment Approach.** Define an approach to identify, evaluate, and treat risks faced by the organization. This methodology, for Argus, is defined in "ISMS-EE-P003: Risk Assessment Policy" and "ISMS-EE-R001: Risk Assessment Process".
1.4	EDH	**Identify Risks.** Identify the risks by following the approach from the previous step. This involves identifying the information assets of the organization, threats to them, their vulnerabilities, and the impact of the threats. For Argus, the risks are documented in "ISMS-EE-D002: Argus Risk Profile".
1.5	EDH	**Analyze Risks.** Analyze and evaluate the risks from last step. Establish the risk

Argus: Retrospection

Project Statistics

- Scope: NSCL Electronics Department
- Time:
  - Start: August 2009
  - Expected End: Early 2012
- Effort (in Person Hours)
  - Planned: ~1000
  - Current: ~800
- Cost :
  - Audit: Approximately 30,000.00 USD
    - Pre-Assessment
    - Stage I & II External Audits
    - Two Post-certification Audits (Yearly)

Current Status

- Completed
  - Risk Assessment
  - Statement of Applicability
  - Initial Set of Documentation
  - Selection of Registrar
- Ongoing
  - Vetting of Policies and Procedures (Documentation)
  - Initial Stages of Implementation
- Expected
  - Internal Audit: Nov 2011
  - External Audits: Dec 2011
  - Certification: Early 2012

Challenges

- Control System Design
- No Encryption, Authentication, Authorization
- Secure Software Development Practices
- PLC Hardening
- Cabling, Password Aging, Employee Agreement
- Culture
- Open Research and Education Environment
- Organizational Changes
- Interest Level: Non-technical and Mundane Work

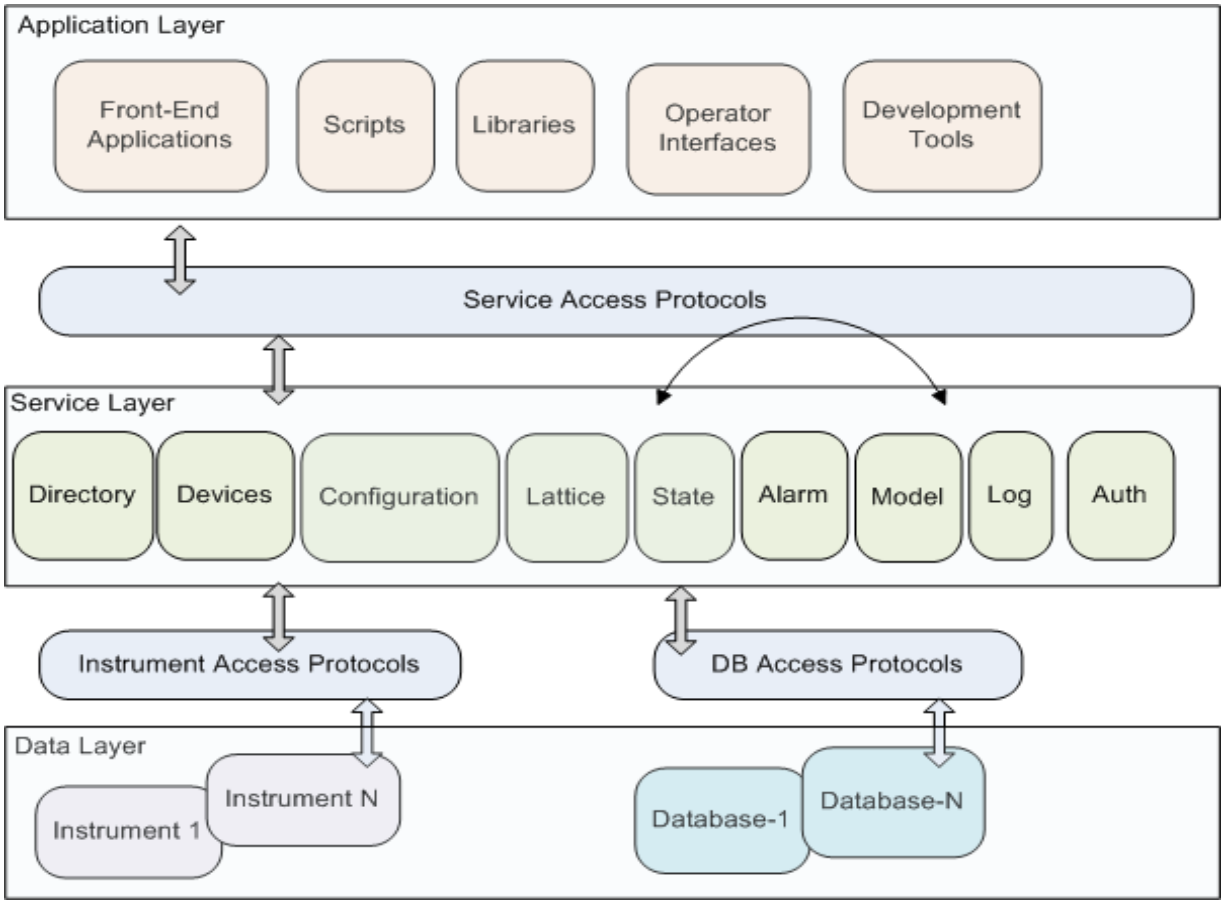
Lessons Learnt I

- Start Small. Implement. Expand.
  - Not Necessary to Include the Whole of IT
  - Use Existing Processes. Do Not Make Drastic Changes
  - Use Small Iterations
- Leverage Existing Management Systems
  - ISO 9001, 14001, 18001,…
- Reserve Resources, If Possible
- Management Support is Crucial
- Don't Lose Focus or Morale
- Needs Support From Every Unit in the Organization
- Define What You Have, Then Go For Best Practice

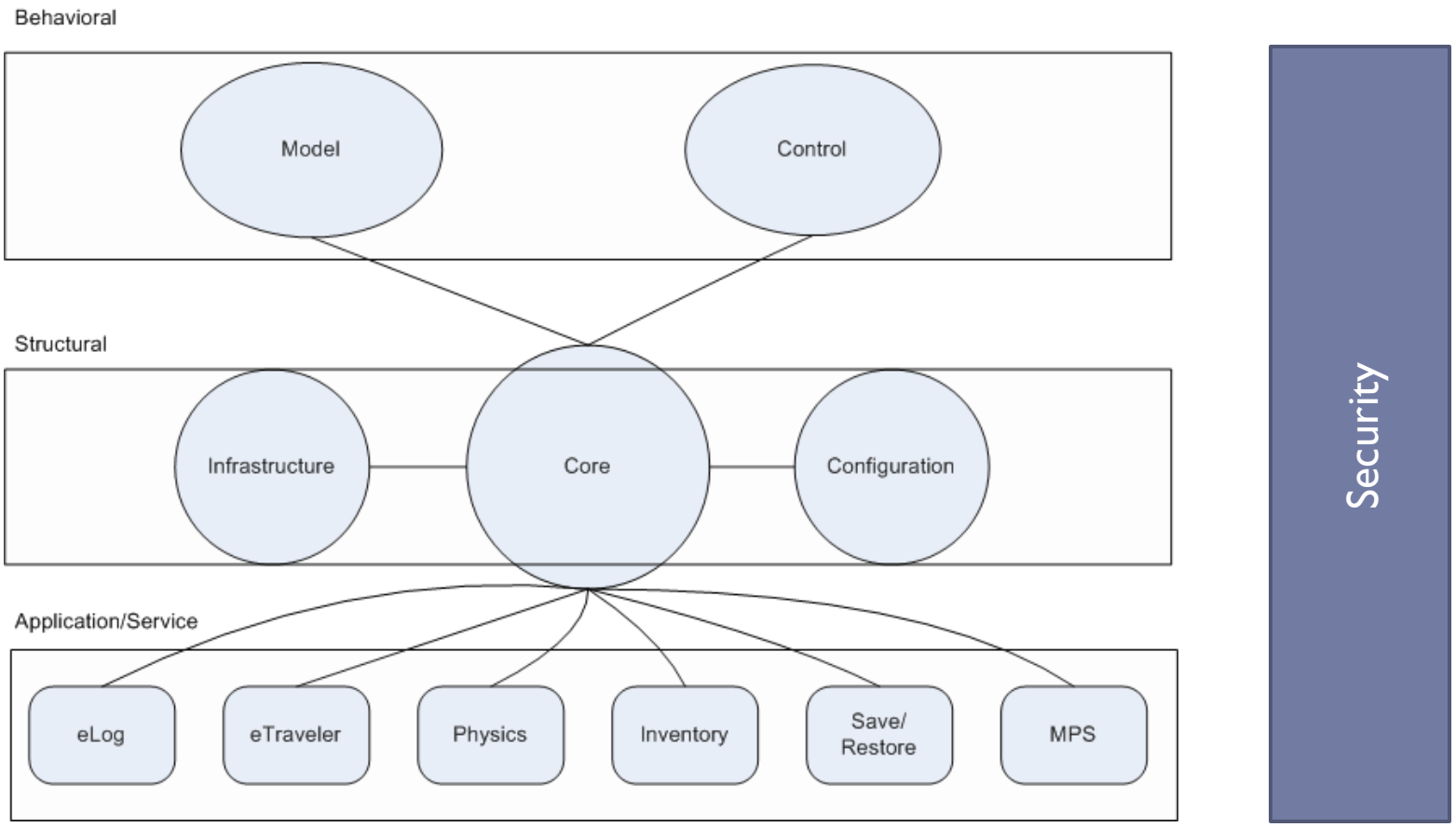
Lessons Learnt II

- Infrastructure
  - Document Management System
  - Incident Reporting/Management System
  - Training System

Control System Information Architecture



FRIB Database Architecture



FRIB Data Security

- Structural
  - Who Can Modify Attributes of a Cavity?
  - Area Based Component Hierarchy
  - Access Control on Areas
- Behavioral
  - Who Can Modify the Voltage (PV) on a Power Supply?
  - Operations Based Component Hierarchy
  - Access Control on the Operations Elements
  - Standalone 'Reserve/Release' Application
  - Not Very Clear How to Implement it on EPICS
    - Modify IOC db Files. IOCs Reload db Files
- Application
  - Who Can Write to Operations LogBook?

Conclusions

- Started as a Small Technical Problem and Grew to a Large Project
- What did we gain?
- Understanding of our Vulnerabilities, Threats, and Risks
- Change in Culture
- Security in Architecture
- References
  - ISO/IEC 27001
  - ISO/IEC 27002
  - ISO 27k Toolkit
  - OCTAVE Allegro

NSCL

Thank you!

"We spend our time searching for security and hate it when we get it." - John Steinbeck