SECURING A CONTROL SYSTEM: EXPERIENCES FROM ISO 27001 IMPLEMENTATION*

V. Vuppala, J. Vincent, J. Kusler, K. Davidson, NSCL, East Lansing, MI 48824, USA.
vuppala,vincent,kusler,davidson@nscl.msu.edu

Abstract

Recent incidents of breaches, in control systems in specific and information systems in general, have emphasized the importance of security and operational continuity in achieving the quality objectives of an organization, and the safety of its personnel and infrastructure. 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 a control system becomes much more difficult during operations.

In this paper we describe our experiences with implementing ISO/IEC 27001 Standard for information security at the Electronics Department of the National Superconducting Cyclotron Laboratory (NSCL) located on the campus of Michigan State University (MSU). We describe our risk assessment methodology, the identified risks, the selected controls, their implementation, and our documentation structure. We also report the current status of the project. We conclude with the challenges faced and the lessons learnt.

INTRODUCTION

NSCL's distributed control system uses Experimental Physics and Industrial Control System (EPICS), and is managed by the Electronics Department (EE). While attempting to secure the control system, it became evident that it could not be done in piecemeal fashion. Hardening one part of the system does not suffice; the weaker links in the chain are either obscured or ignored, and leave the entire system as vulnerable as before. So EE wanted to address security in a holistic manner, and decided to implement the ISO/IEC 27001 Standard for information security.

Confidentiality, Integrity, Availability

The cornerstones, basic principles, or foundations of information security are Confidentiality, Integrity, and Availability (CIA). Confidentiality ensures that only authorized personnel have access to information. Integrity ensures that the information remains valid by guarding against unauthorized modifications and destruction. Availability guarantees that the information is available whenever requested (by authorized personnel).

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

ISO/IEC 27000 STANADARDS

ISO/IEC Standard 27001 and 27002 form the crux of the 27000 series of standards. ISO Standard 27001 (based on British Standard 7799 Part 2) provides guidance to establish, implement, operate, review, and improve an Information Security Management System (ISMS). ISO 27002 (based on British Standard 7799 Part 1) describes the best practices to manage information security risks. ISO 27001 presents a management system: a framework of policies, procedures, guidelines and associated resources to achieve the security objectives of the organization. ISO 27002 presents a set of controls: means to manage security risks.

ISO 27001 advocates an iterative process-based approach built on Plan-Do-Check-Act (PDCA) model to establish and manage an ISMS [1]. It recommends four phases for ISMS: establish, implement and operate, monitor and review, and maintain and improve. It mandates management responsibilities, internal audits, reviews, and continuous improvement of the ISMS.

ISO 27002 is divided into eleven clauses [2]. Each clause is divided into categories. Each category has an objective and a set of controls to achieve that objective. The security clauses in ISO 27002 are:

- Security Policy
- Information Security Organization
- Asset Management
- HR Security
- Physical Security
- Communication and Operations Management
- Access Control
- Information Systems Acquisition, Development, and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance

An organization is certified against ISO 27001 and not ISO 27002. Annex A of ISO 27001 refers to the controls of ISO 27002.

ARGUS THE ISMS

In this section we describe the implementation of Argus, our ISMS. Its roadmap is shown in **Figure 1**. We first defined Argus' scope (it was limited to the EE department and related support services), and the guiding policy for the ISMS. Next we chose the OCTAVE Allegro [3] as our risk assessment methodology. Using this approach we identified our critical information assets:

information that is important to us. This included controls and PLC software, documentation of our systems, software licenses, EPICS archiver database, and IOC configurations. Then, we identified the containers of the information assets. The containers can be of three categories: technical (server, software, hardware etc), physical (paper, folders etc), and human (intellectual property, ideas etc).

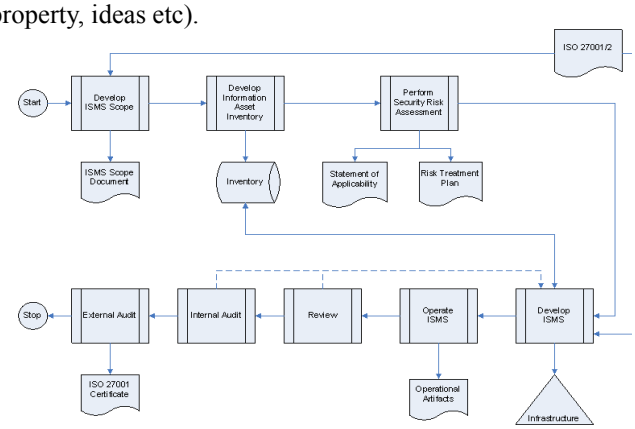

Figure 1: Argus Roadmap.

Risk Assessment

As the next step, we identified the conditions (areas of concern) that can affect the information assets or their containers. Then we qualified them with actors, means, and outcomes. This resulted in a list of threats to our assets. An example of such threat is: anyone with access to control network can modify the IOC configuration files. We then evaluated the impact (see Table 2) of every threat based on a set of measurement criteria (

Table 1). This gave us a relative risk score (RRS) for each risk. An example of this score is shown in Table 3 for the risk - "inadvertent modification of EPICS channel values".

Table 1: Risk Measurement Criteria

Impact Area (IA)	IA Priority
Safety and Health	5
Reputation	4
Financial	3
Legal	2
Productivity	1

Table 2: Impact Values

Impact	Value
No Impact	0
Low	1
Medium	2
High	3

Table 3: Relative Risk Score for a Risk

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

We used the RRS to prioritize the risks. . Based on the relative risk score and probability of risk occurrence, we could categorize the risks into various levels. An example of such risk level matrix is shown in Table 4.

Table 4: Risk Levels

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

We treated the risks based on the risk level or priority. Risk treatment involved one of the following actions:

- Avoid the risk by using the controls from ISO 27002 or controls developed in-house
- Reduce the risk by using the controls
- Accept the risk or residual risk. If the risks are of low probability and incur high cost for mitigation, they may be accepted. However, all acceptable risks must be documented and approved by EE department head.
- It is possible to transfer a risk by insuring against it but we did not have any such risks.
- It is also possible to share risks, with vendors of other labs, but we did not encounter such risks.

Documentation

Documentation forms a critical part of any management system. The policies, procedures, standards, and guidelines related to Argus are structured in a hierarchical fashion. Policies refer to related procedures which in turn point to relevant guidelines, standards etc (see Figure 2). The top level policies and procedures are linked together in the *Argus Security Handbook*. The existing document system used by the lab for ISO 9001, 18001, and 14001 management systems is also being utilized for Argus' documentation.

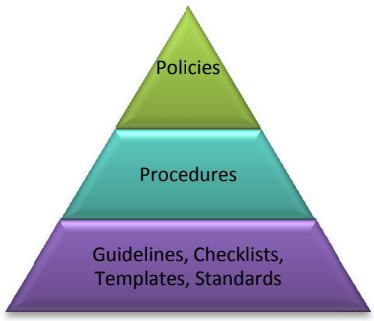

Figure 2: Argus Documentation.

		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					

Figure 3: Access Control Matrix.

ARGUS CONTROLS

The controls used in Argus are identified in Argus Statement of Applicability. A security policy for the department and a policy for its periodic review were defined. An organization structure is put in place to focus on information security and management of Argus. It consists of Information Security Board, IT Group, and Information Security Manager. The EE department head leads this organization. The physical and human resource security policies and procedures are based on current practices which were found to be adequate. For disaster recovery, the backup tapes are taken off-site on a weekly basis. A mechanism for live off-site backups, to a remote facility, is being implemented. Business continuity plans and procedures are defined but not tested. Many of the standard operations and communications management controls were found to be adequately covered by the current practices; the rest were implemented.

The current Trouble Reporting System used for the existing ISO based management systems (9001, 18001, and 14001) is being utilized for security incident management. Legal, statutory, and contractual compliance policies are based on NSCL's and MSU's policies.

The existing software development and project management policies and procedures were incorporated into Argus. New policies and guidelines on secure software development practices were developed.

Access Control

The information assets were classified into five categories, Class I through V, Class I being the most sensitive and Class V being least sensitive. Information assets in the department can be accessed through various means: Internet, Michigan State University Wired or Wireless Network, NSCL Controls Network, NSCL Office Network etc. Access controls were defined based on the information class and access method. An example access control matrix is shown in Figure 3. To improve security, the various networks within the lab were segregated, through a firewall, at the end of last year.

ARGUS LIFECYCLE

Argus is a living system; it continuously improves itself through reviews, audits, and feedbacks. The phases and activities of its lifecycle, defined in *Argus ISMS Policy* and *Argus ISMS Procedure*, are summarized below.

- 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
- 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

RETROSPECTION

Challenges

Control Systems have been designed, by vendors and the community, with little emphasis on security. They are not designed to guard against malicious code or unauthorized access. So they have to be secured through external means such as management procedures, user training, and network isolation. It is also difficult to harden control system platforms such as PLCs. We found that it is difficult to implement secure software development processes. Programmers should understand and guard against security issues like buffer overflows,

memory leaks, SQL-injection etc which add to their programming effort. Static and dynamic source code analysis tools are useful but require programmers to learn to use them.

The educational and research oriented environment in the lab is also not favourable for implementing security procedures. Changing the culture of the organization is a challenge. Security conflicts with convenience, and finding the balance is difficult.

Lessons Learnt

ISO 27001 is an extensive standard; implementing it is an onerous task. However, it is not necessary to implement it across the entire organization in one shot. The standard allows the scope to be adjusted. Hence, it is crucial to start small, implement it, and then expand. For the initial iteration, start with the current practices, document them, establish the initial ISMS, and them improve upon it. Do not make drastic changes to the current processes; this will only infuriate the users. Remember, users are an important, if not the most important, part of the overall security system.

The most important factor for the successful implementation of any management system, especially ISO 27001, is management support. Without it, the required changes to the organization's culture are impossible.

Leverage the infrastructure of existing management system like ISO 9001. There are several similarities among these standards, which allow the infrastructure and processes to be shared.

ISO 27001 implementation requires support from every unit of the organization, so involve all the units in the process especially during risk assessment. We made a deliberate decision not to use consultants to help us with the implementation. An in-house team is required to manage the ISMS. The consultant may help with the templates and guidance, however bulk of the work still needs to be done by the in-house team. It is worthwhile to train the in-house team in ISO 27001 audit and related trainings.

ARGUS PROJECT

Risk assessment, Statement of Applicability, Risk Treatment Plan, and initial set of documentation have been completed. The registrar for external audit has been selected through a formal bidding process. The external audit of Argus comprises of pre-assessment, Stage I audit, and Stage II audit. The Argus documents are currently being vetted. Internal audit and pre-assessment are expected to be completed by end of 2011.

The project to develop Argus was started in August of 2009; it is expected to finish in the early 2012. The estimated effort was approximately 1000 person hours, of which approximately 800 have been currently spent.

CONCLUSION

. Was the implementation worth the effort and cost? We think so. Due to this exercise, we have a very good insight into our vulnerabilities, threats, and risks. This experience has helped us incorporate security as a design element in the development of our systems. The original intent was to eventually expand this to the rest of the lab. Even though this implementation was not a requirement from our current customers, we feel that it will eventually attract more security-sensitive projects to the lab.

REFERENCES

[1] ISO/IEC 27001 International Standard, Information Technology – Security Techniques – Information security management systems – Requirements

[2] ISO/IEC 27002/17799 International Standard, Information Technology – Security Techniques – Code of practice for information security management

[3] The OCTAVE Allegro Guidebook V1.0, Computer Emergency Response Team (CERT) Program, Software Engineering Institute, Carnegie Mellon University

[4] ISO 27001 Toolkit, http://www.iso27k.com