An Outsider's Look at Information Security Management in Libraries, Museums, and Archives (LMAs)

Allan August P. Malig, CISSP
PJ Lhuillier Group of Companies

Abstract. The paper aims to provide an outsider's perspective on how long established and widely accepted information security management practices can be applied in Libraries and Museums. It includes an overview on basic information security management concepts, risk assessment approach and practical tips to ensure basic information security hygiene practices are in place. Finally, it provides an overview on ISO 27001-an international standard for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System.

Keywords: Information Security Management, Risk Management, International Organization for Standardization/International Electro technical Commission [ISO/IEC] 27001, ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 1799

I. Introduction

Information Security (IS) is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities. (ISO/IEC 17799:2005, viii). Information Security primarily concerns itself with the preservation of three (3) properties of assets namely confidentiality, integrity, and availability (also known as the C.I.A Triad). ISO/IEC 27001:2005 defines Confidentiality, Integrity and Availability in the following manner:

Confidentiality: Property that information is not made available or disclosed to unauthorized individuals, entities, or processes (p. 3). For instance, only authorized LMA personnel and systems should have access to information about employees, donors, and visitors.

Integrity: Property of safeguarding the accuracy and completeness of assets (p.3). For instance, information stored in OPAC or Library Catalogs should be accurate and complete at all times.

Availability: Property of being accessible and usable upon demand by an authorized entity (p. 3). For instance, an LMA's official web site should be accessible 24/7 with all service maintenance windows announced seven (7) days before.

What keeps you awake at night?

This is the top of mind question one would ask when tasked to assess the information security requirements of an organization for the first time. Responses received can be very insightful particularly when answered by experienced practitioners, managers, or administrators. More often than not, the following concerns will be mentioned:

- **Physical Security/Management of Facilities**

  Physical security is a concern in particular for organizations with handling valuables such as cash, jewelries, priceless collections, and commercial goods. The same can be said for organizations where the threat from terrorist attacks is material.

  Maintenance of facilities such as cooling, power, heating, humidity, fire suppression, and pest control is also an important concern for organizations with climate controlled facilities such as those used to house computer data centers or LMA exhibits.

- **Natural Disasters**
  Natural disasters such as flooding, earthquakes, tsunamis and pandemics can affect any type of organization. Inability to prepare and respond to disasters may adversely impact the safety of personnel and continuity of operations.

- **External Threats**
  Attacks from the outside directed towards an organization's Information and Communications Technology (ICT) infrastructure or, at times, its people may result in a myriad of problems such as unauthorized disclosure/alteration of information, system downtime, fraud, identify theft and system break-ins ("hacking").

- **Internal Threats**
  Internal threats may include attempts by personnel with malicious intent to defraud, steal/alter information, disrupt operations, or discredit the organization. In some cases though, the intent may not be malicious at all. For instance, accidents such as unintentional deletion/alteration of information or introduction of untested changes may yield the same results.

- **Virus or Malware**
  Malware or malicious software attacks may result in unauthorized disclosure of information, denial of services, or system downtime. The Internet is now considered a major source of malware infection. In some cases, even legitimate sites can be infected with malware that can be downloaded to connecting computers. According to SophosLabs (2011), more than 30,000 websites are infected every day and 80% of those infected sites are legitimate.

  In some cases, sophisticated malware such as the Stuxnet worm (Sophos, 2011, p. 5) appears to have been designed to attack very sophisticated and critical SCADA (Supervisory Control and Data Acquisition) systems. These systems are generally used by critical public utility providers such as power plants, transportation, and water treatment facilities.

- **Mobile Computing Devices**
  Mobile devices such as smart phones and laptops have added flexibility and mobility to an organization. However, their small size makes them prone to loss or theft which, in turn, may result in disclosure of information. These devices can also be used to discreetly break into our networks, particularly the wireless ones. Furthermore, these devices can also be used to secretly take pictures and videos or record conversations. Loss of productivity (i.e. playing of games during work hours) may also be a concern for some organizations.

- **Social Networking**
  The online press room of Facebook® estimates that there are about 955 million active users as of June 2012. It is for this reason why social networking sites such as Facebook is a prime target for individuals or organizations with malicious intent such as criminals, malware developers, scam artists, and unscrupulous online marketers. According to the 2011 Sophos Threat Report:

  > **Click jacking uses the standard arsenal of social engineering techniques to lure new victims and trick them into clicking on the disguised links, many of which developed a rather dark tone in 2010. Alongside the usual barrage of lures such as humor, compromising pictures of celebrities and major news and entertainment events, we saw a rise in increasingly bizarre and often gruesome content. Stories of suicide, car crashes, and shark attacks, the allegedly "horrific" effects of a popular drink and over-the-top revenge stories were all click jacking scams in 2010.**

  Sophos also stated that aside from spreading unsolicited messages or advertisements, actions such as granting access to personal information and, in some cases, even unauthorized online purchases may take place as well. Too much information shared over social networking sites may also result in information disclosure -intentional or otherwise.

- **Removable Media**
  Nowadays, USB flash drives, which can easily store information by the Gigabytes, are easily accessible and available at a cheap price. People with malicious intent can use it to download and steal information. Malware developers also use it to distribute malware. For instance, malware strains such as Conficker (Sophos, 2012, p. 16) takes advantage of the AutoPlay feature which allows it to install itself onto the computer when the flash drive is inserted to a USB port.

- **Social Engineering**
  Social Engineering is a collection of techniques used to manipulate people into performing actions or divulging confidential information (McKinley, 2012). Social Engineering is designed to attack us, technology users who are considered as the weakest link. Such techniques may include a caller pretending to be an authority figure and demanding a password be reset or an email enticing a recipient to click on a link (that will download malware) out of curiosity or interest.

- **Hacktivism**
  www.mashable[dot].com defines hacktivism as the use of computers and computer networks as a means of protest to promote political ends. Hacktivists typically deface sites, redirect traffic, divulge confidential information (Sophos, 2012, p. 4) or bombard a web site with network traffic, which will render it inaccessible to legitimate users. One such group said to be involved in hacktivism is called Annonymous, whose prime targets are governments and large multinational companies. In recent events, Annonymous Philippines defaced the sites of Philippine institutions such as the central bank, the health department, a water utilities company, and a chamber of commerce as an act of protest against the enactment of the Cybercrime Prevention Act of 2012 (Diola & Magtulis, 2012, paragraph 2).

II. Information Security Risk Management

Threats and Vulnerabilities

A very important aspect of IS Management is assessing and managing IS risks. In fact, Information Security Management is all about managing risks. Risk is the potential that given threat will exploit vulnerabilities of an asset or group of assets thereby causing harm to the organization (ISO/IEC 27005:2008, p. 1). Two key concepts are mentioned in this definition, namely threats and vulnerabilities. Threat is a potential cause of an unwanted incident which may result in harm (ISO/IEC 17799: 2005, p. 1). On the other hand, vulnerability is a weakness of an asset or a group of assets that can be exploited by one or more threats. (ISO/IEC 17799: 2005, p. 1) Table 1 shows examples of assets and corresponding threats and vulnerabilities.

Table 1: Examples of Assets, Threats, and Vulnerabilities

Asset Type	**Asset Example**	**Threats**	**Vulnerability**
Information	Databases of collections, visitors, employees, and patrons	Information disclosure	Lack of policy for handling confidential information
Software	Database Management System	Abuse of access privileges	Program bugs
Physical Assets	Collections/Exhibits	Pests	Lack of environmental controls on cleanliness, temperature, humidity, etc.
People	Personnel with specialized skills such as curators, restorers, and translators	Resignation	Lack or insufficient motivation
Site	Climate-controlled rooms for priceless collections or artifacts	Loss of power stable	Substandard cabling practices
Services	Local Area Network Facilities	Failure of networking equipment	Substandard cabling practices

Intangibles	Reputation	Lawsuits	Lack of communications policy

Reference: ISO/IEC 17799:2005

Establishing an inventory of assets along with identification of applicable threats-vulnerability is the first important step in IS risk management.

Asset Value, Probability, Impact, and Risk Rating

The next step in IS risk management involves coming up with a way to quantify and/or qualify IS risks so that the risks can be ranked according to criticality. With finite resources (allotted to IS initiatives), establishing the risk ranking priority will help the organization determine what asset-threat-vulnerability combination needs to be addressed first. Moreover, prioritizing high-risk items will help bring down the overall IS risk profile of the organization.

In assessing the criteria for a risk rating, three important factors are generally considered:

Asset Value: This refers to the assessed worth or monetary equivalent (if applicable) of an information asset. An example of an Asset Value Scale is shown in Table 2.

Table 2: Asset Value Scale Example

Scale	**Description**
Low (1)	Up to 20K USD Commercially available locally
Medium (2)	Above 20K up to 50K USD Commercially available outside the country
High (3)	Above 50K USD Rare or one of a kind

Probability: This refers to the likelihood of an unexpected or uncertain occurrence of an event. An example of a probability scale is shown in Table 3.

Table 3: Probability Scale Example

Scale	**Description**
Low (1)	Likely to occur in a ten (10) year period; has not occurred; unlikely to take place
Medium (2)	Likely to occur in a five (5) year period; has a history of occurrence
High (3)	Likely to occur each year; has occurred recently

Impact is related to the degree of success of an incident (ISO 27005:2009, p. 38). It is also an evaluation of the extent or severity of damage. Unlike in probability, which is generally expressed in a time period scale, impact considers multiple scales, depending on what aspect of the organization is affected. Table 4 shows a sample matrix for assessing impact on financials, operations, people, or system availability.

Table 4: Impact Scale Matrix Example

Scale	**Impact on Financial**	**Impact on Operation**	**Impact on People**	**Impact on System Availability**
Low (1)	Loss of up to 20K USD	Limited to one section or department only	Minor injury to an individual	Less than an hour
Medium (2)	Loss is above 20K USD to 50K USD	More than 1 department is affected	Minor to several or major injury to an individual	More than an hour to 4 hours
High (3)	Loss is above 50K USD	Entire Organization affected	Major injuries/death	More than 4 hours

The next step would be to assess the (asset) value, impact, and probability of an information asset with respect to a specific threat-vulnerability pair. This will be based on the experience of the organization in order to arrive at the risk rating score as shown in table 5 below. The formula used is **Risk Rating** = Asset Value X Probability X Impact.

Table 5: Risk Rating = Asset Value X Probability X Impact

Asset Example	Threats	Vulnerability	Asset Value	Probability	Impact	Risk Rating
Databases of collections, visitors, employees, and patrons	Information disclosure	Lack of policy for handling confidential information	3	2	2	18
Database Management System	Abuse of access privileges	Program bugs	2	2	3	12
Collections/Exhibits	Pests	Lack of environmental controls on cleanliness, temperature, humidity, etc.	3	3	3	27
Personnel with specialized skills such as curators, restorers, and translators	Resignation	Lack of insufficient motivation	3	1	2	6
Climate-controlled rooms for priceless collections or artifacts	Loss of stable power	Unstable power source grid	3	1	3	9
Local Area Network Facilities	Failure of networking equipment	Substandard cabling practices	2	1	2	4
Reputation	Lawsuits	Lack of communications policy	3	2	3	18

A rating scale similar to Table 6 can be used to describe the resulting risk rating scores qualitatively.

Table 6: Risk Rating Scale Example

Scale	Description
Low (1)	Risk Rating of 9 and below
Medium (2)	Higher than 9 but less than 18
High (3)	18 or higher

The resulting list can then be sorted according to risk rating scores similar to Table 7. Generally, attention and resources will be focused on addressing the high-risk items.

Table 7: Assets sorted according to Risk Rating Score

Asset Example	Asset Value	Probability	Impact	Risk Rating	
Collections/Exhibits	3	3	3	27	High
Databases of collections, visitors, employees, and patrons	3	2	2	18	High
Reputation	3	2	3	18	High
Database Management System	2	2	3	12	Medium
Climate-controlled rooms for priceless collections or artifacts	3	1	3	9	Low
Personnel with specialized skills such as curators, restorers, and translators	3	1	2	6	Low
Local Area Network Facilities	2	1	2	4	Low

The organization must then decide on the risk reduction strategy to be used. Risk reduction refers to actions taken to lessen the probability, negative consequences, or both, associated with a risk (ISO 27005: 2008 p. 2). Table 8 compares the different risk reduction strategies as discussed in ISO 27005: 2008:

Table 8: Comparison of the different risk reduction strategies

Asset Example	Reduce the Risk	Retain the Risk	Avoid the Risk	Transfer the Risk
Asset: Collections/Exhibits **Threat:** Pests **Vulnerability:** Lack of environmental controls on cleanliness, temperature, humidity, etc. **Risk Rating:** High (27)	***Reduce risk level by selection of controls so that residual risk can be reassessed to acceptable levels*** "Strictly enforce no food and drinks policy inside the exhibit areas"	***No further action taken. Risk is within acceptable levels*** "The exhibits will not be harmed or damaged by the pests. If damaged, we can replace easily"	***Activity or condition that gives rise to the risk should be avoided*** "Exhibit with pest infestation will be closed"	***Transfer risk to another party or organization*** "Outsource pest control to a third party" or "Move the exhibit to another museum"

The rating scales used to represent asset value, impact, probability, and risk rating may vary and can be customized to satisfy the (granularity) requirements of an organization. However, it is important for the same rating scales to be used across the entire organization to ensure consistency in results and interpretation.

III. ISO/IEC 27001: 2005 and ISO/IEC 17799*

ISO/IEC 27001: 2005 is a model for establishing, implementing, operating, reviewing, maintaining, and improving an information security management system (ISMS) (ISO/IEC 17799: 2005, viii). It can be used as the basis for setting up the ISMS within an organization. As a process, it is based on the PDCA (Plan-Do-Check-Act) model made popular by Dr. W. Edwards Deming, and it should be best looked at as a cycle for continuous improvement. Figure 1 illustrates the application of the PDCA cycle in ISMS as presented in the ISO 27001:2005 standard manual.

* ISO/IEC 17799:2005 is now known as ISO/IEC 27002: 2007. (Arnason & Willet, 2007, p. 25).

Figure 1: P-D-C-A Cycle

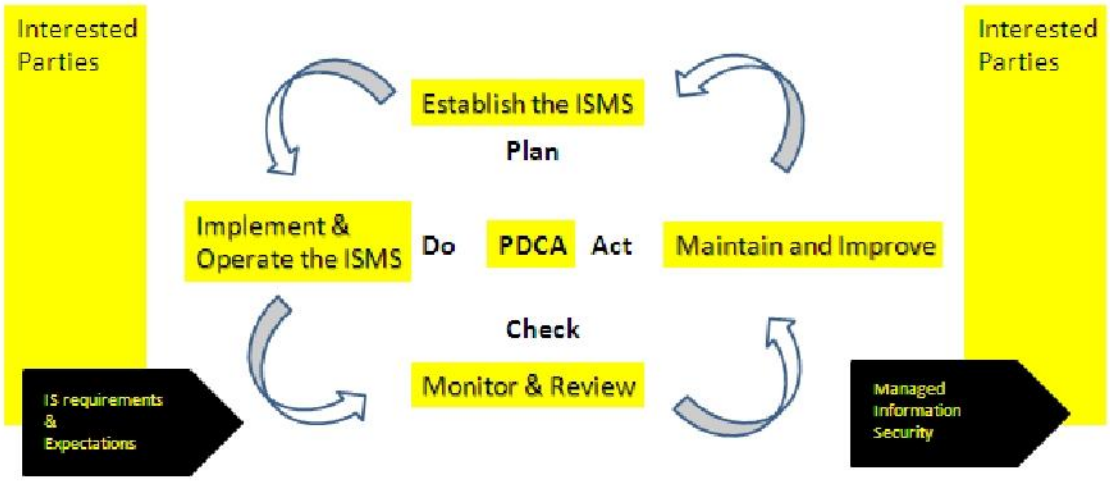

Table 9 provides a high level overview of the primary activities per phase within the ISMS PDCA cycle as presented in the ISO 27001:2005 standard manual.

Table 9: Activities per phase of the ISMS PDCA cycle.

Plan **Establish the ISMS**	Establish the ISMS policy, objectives, processes, and procedures relevant to managing risk-improving information security to deliver results in accordance with an organization's overall policies and objectives.
Do **Implement and Review the ISMS**	Implement and operate the ISMS policy, controls, processes, and procedures.
Check **Monitor and Review the ISMS**	Assess and, where applicable, measure performance against ISMS policy, objective, and practical experience, and report the results to management for review.
Act **Maintain and Improve the ISMS**	Take corrective and preventive actions based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.

ISO 27001 contains an annex of control objectives and controls which can be implemented to address risks identified during assessment. A **control or countermeasure** is defined as a means of managing risks such as policies, procedures, guidelines, practices, or organizational structures, which can be of administrative, technical, management or legal in nature (ISO 17799: 2005, p.2). The following is an example:

Control Objective: Responsibility for Assets (A.7.1 under Section A.7 Asset Management) "To achieve and maintain appropriate protection of organizational assets"
Sample Controls: 1. Inventory of Assets: All assets shall be clearly identified and inventory of all important assets drawn up and maintained. (A.7.1.1) 2. Ownership of Assets: All information and assets associated with information processing facilities shall be "owned" by a designated part of the organization. (A.7.1.2)

ISO 27001 is complemented by ISO 17799:2005 by elaborating on implementation guidelines of the controls specified in the former standard. For instance, the following is an excerpt of the implementing guidelines provided by ISO 17799 to ISO 27001's Asset Management objective.

Control Objective: Responsibility for Assets (A.7.1 under Section A.7 Asset Management) "To achieve and maintain appropriate protection of organizational assets"
Sample Controls: 1. Inventory of Assets: All assets shall be clearly identified and inventory of all important assets drawn up and maintained. (A.7.1.1) 2. Ownership of Assets: All information and assets associated with information processing facilities shall be "owned" by a designated part of the organization. (A.7.1.2)
Implementation Guidelines: Inventory of Assets as detailed in ISO 17799 An organization should identify all assets and document the importance of these assets. The asset inventory should include all information necessary in order to recover from a disaster, including type of asset, format, location, backup information, license information, and business value. Types of information include: • Information such as databases and data files, contracts, etc. • Software such as operating systems and application systems • Physical Assets such as computer equipment and removable media • Services such as computing service or general utilities • People and their qualification and skills • Intangibles such as reputation

IV Conclusion

Managing Information Security is a common challenge faced by any organization tasked with safeguarding information assets. Establishing an ISMS can be an overwhelming experience, but international standards such as ISO 27001and ISO 27002 make it more manageable by providing the process framework and controls needed to jumpstart the implementation.

In summary, it is recommended that following should be considered and prioritized when establishing an ISMS.

Establish Tone from the Top
Winning the support of an organization's top management is the key to any initiative including establishing an information security management system. This helps in delivering a clear message that information security is included in the organization's top priorities and everyone, regardless of rank or position should, be involved in achieving its (information security) objectives.

Keeping management informed about the current state of information security within the organization is equally important. All major initiatives should be presented to management for approval.

Documented Policies
Policies, standards, and work instructions should be documented, approved, and disseminated accordingly. Documentation helps promote consistency and continuity of implementation.

Risk Assessment
Performing risk assessment will help identify areas that need to be prioritized. Risk assessment results should be communicated and approved by management. Risk Assessment should also be performed on a regular basis since risks may change over time.

Training/Awareness
Training/Awareness addresses the human factor within any organization. It will promote information security by keeping management, employees, third party contractors, and even visitors informed enough to appropriately respond to potential security concerns that they may face. It will also promote observance of basic security practices and help reduce incidents particularly those committed out of ignorance or lack of proper training.

Observance of Basic Security Hygiene
The following preventive security practices ("Basic security hygiene practices") will be instrumental in minimizing information security threats. Proactive measures are more cost effective than reactive measures in response to security incidents.

- Use of updated anti malware software;
- Regular monitoring and preventive maintenance of hardware;
- Keeping software updated and hardened (i.e. all unnecessary services and applications are turned off); and,
- Observance of the principle of least privilege (i.e. access is granted is determined by function or need and not by position or stature in the organization)

Information Asset Ownership
Establishing ownership for information assets is needed to ensure assignment of responsibilities particularly for the maintenance and enforcement of controls to protect the information assets.

Enforcement
Strict enforcement of information security policies is crucial in managing information security within the organization. It delivers the message that the organization will not tolerate any attempts to circumvent any policies in place. Close coordination with the organization's respective human resources and legal teams is needed since penalties/sanctions should be in accordance with the organization's established code of conduct and applicable laws.

Auditing/Third Party Assessment
An independent assessment of an organization's information security management system will help in validating implementation and enforcement of policies and controls in place. It will also assist in identifying additional areas for improvement and even discover fraud (if any). It also helps boost the morale and confidence of the team handling information security particularly when the installation passes audit or third party assessment.

References

Arnason, Sigurjon & Willet, Keith. How to Achieve ISO 27001 Certification. (Auerbach publications, © 2007).

Diola, Camille & Magtulis, Prinz. Anonymous Philippines' on a hacking spree (September 27, 2012). www.philtstar.com.

Facebook. Online Press Room. Retrieved Sept 5, 2012 from www.facebook[dot]com.

Hacktivism. (2012). Retrieved September, 2012, from www.mashable.com

ISO/IEC 17799:2005. Code of Practice for Information Security Management. (Published in Switzerland, ©2005)

ISO/IEC 27001:2005. Information Security Management System. (Reprinted by Department of Trade and Industry - Bureau of Product Standards [DTI—BPS] as a Philippine National Standard [PNS] ISO/IEC 27001:2006).

ISO/IEC 27005:2009. Information Security Risk Management. (Reprinted by Department of Trade and Industry - Bureau of Product Standards [DTI—BPS] as a Philippine National Standard [PNS] ISO/IEC 27005:2009).

McKinley, Michael. Social Engineering Threats: Tales from the Trenches. Presented during Information Security Consortium Security Congress 2012 Conference. (September 10-13, 2012, Philadelphia, PA).

Sophos Ltd. Sophos Security Threat Report 2012. www.sophos.com (© 2012).

Sophos Ltd. Sophos Security Threat Report 2011. www.sophos.com (© 2011).

About the Author

Upon graduating from the University of the Philippines Diliman with a degree in BS Education major in Social Studies, Allan started the first 5 years of his ICT Career as an IT instructor and, eventually, as courseware development supervisor for Systems Technology Institute. He then moved on to Equitable PCI (EPCI) Bank where he helped establish and manage the Technology Training Center of its IT Group. In 2001, he embarked on his Information Security career when he helped establish and manage the Information Security Office of EPCI. In 2004, he became the Information Security Manager at the Sun Life Financial for its operations in the Philippines, Indonesia, Hong Kong, China, and India. He also spent 2 years leading the IT/Security Internal Audit Cluster of Globe Telecoms. Since 2008, he has been the head of Information Security and IT Governance Division for the PJ Lhuillier Group of Companies where he is tasked with leading all initiatives and operations related to Information Security, Change Management, IT Quality Assurance, and Enterprise Business Continuity Planning.

Allan is a Certified Information Systems Security Professional (CISSP) since 2005 and a passer of the Certified Information System Auditor (CISA) exam in 2008.