Information Security Risk Management Program – Program Essentials

By Dean Choudhri, CISSP, Manager, Information Security Risk,*
Alloya Corporate FCU
dean.choudhri@alloyacorp.org

The current information technology (IT) landscape is changing at a rapid rate as new technologies are brought to market, legacy systems are decommissioned and new regulatory requirements are enacted. The dynamic nature of IT also introduces new security risks to IT assets. In order to continue to grow and provide competitive products and services, organizations must be able to effectively manage these risks. Incorporating an information security risk management (ISRM) program that utilizes risk assessments into your credit union's information security policy is essential, and can provide the ability to assess the inherent risks to assets when changes are made to the computing environment (e.g. your member base or the information security environment). Recently published guidance from the Federal Financial Institutions Examination Council mandates that credit unions continually assess the risks to their assets and member information.

The goal of an ISRM program is to ensure the confidentiality, integrity and availability (CIA triad) of IT assets. A further explanation of the CIA triad:

Confidentiality – Protecting the confidentiality of systems and data ensures that only authorized users are able to access and use data or systems.

Integrity – Referring to the processes and controls that are in place to ensure changes to systems and/or data are only made by authorized personnel.

Availability **–** Continuous availability of systems and data will ensure that authorized users have consistent and reliable access to information and systems when needed.

The involvement of all lines of business is an important component of a successful ISRM program; however, risk management is ultimately the responsibility of the board of directors and executive management. Their sponsorship of the ISRM program is necessary to ensure program success, and will demonstrate management's commitment to information security.

An ISRM program allows the board of directors or its assignees to:

- Establish an acceptable level of risk and make well informed risk management decisions.
- Determine the potential impact of these risks to the organization.
- Identify information security risks that could prevent the organization or its members from achieving their respective missions.
- Meet regulatory requirements for information security in a cost-effective manner.
- Authorize new systems and technologies that could significantly alter the computing environment.

The success of the ISRM program requires that all individuals involved work collaboratively to identify, assess and mitigate risk. Individuals participating in risk assessments should be empowered to communicate openly and honestly during the process. Finally, business units must understand that the risk assessment process is ***not an audit*** of their processes and procedures, but a means to help protect their assets and achieve their goals in a secure and cost effective manner.

Best Practices for Applying your ISRM

There are standard, proven best practice approaches to information security risk management. The methodology outlined below is consistent with many of these approaches and should be used as guide when assessing risks. If needed, the methodology can be customized to meet specific regulatory or business requirements of your organization.

Identify Assets – Having a comprehensive and current catalog of all information assets is the crucial first step in the risk assessment process. Assets may include, but are not limited to, personnel, hardware, software, data (including classifications of sensitivity, privacy and criticality) and facilities.

Value Assets – Although all assets have some value to the organization, every organization has assets that are critical to helping the organization meet its mission. When assigning value to assets, the following questions should be considered. Does the asset house sensitive data? Would there be a significant impact to the business if CIA were affected? Are there specific regulatory requirements associated with the asset?

Identify Threats – A threat should be thought of as any process, event or action that has the ability to exploit vulnerability. Who or what can do harm to the system? It is important to not only consider threats to the organization, but also threats to members and vendors. Examples of threats:

- Hardware/software failure
- Personnel changes
- Accidental destruction or disruption of access to data
- Environmental (power failure, fire, flood, natural disaster)
- Computer virus
- Internal or external hacker

Identify Vulnerabilities – What weaknesses exist in the system? Vulnerability should be thought of as any weakness in a system, or even an operational function, that a threat may exploit, resulting in negative impact to assets or operations. Vulnerability reports, audit results and any industry-specific notices and alerts should be reviewed to help identify vulnerabilities. Examples of vulnerabilities:

- Lack of redundant systems
- Maintenance procedures not documented
- Insufficient cross training of department personnel

- No alternate power sources, lack of fire suppression equipment
- Anti-virus software not installed or updates not applied
- Lack of data encryption, system security recommendations not implemented

Identify Existing Controls – What protections are in place? Processes, policies, procedures or systems can either reduce the likelihood of a threat that exploits a vulnerability or limit its impact. It is important to identify and catalogue all existing controls that are currently in place. Examples of controls:

- Security policies
- Tape backups
- Monitoring
- Audiovisual software

Determine Likelihood – How likely is it that an identified threat will exploit vulnerability? In order to determine the likelihood of the event happening, you must consider the following:

- How motivated and able is the threat source?
- Is the vulnerability obscure, or has the vulnerability been exploited previously at your organization or other organizations?
- Consider the controls in place and how effective these controls are in decreasing the likelihood of the event occurring.

After considering these points the likelihood can be measured by simply assigning a High, Medium or Low value to each threat.

Determine Impact – What would the impact be to the organization if the threat did exploit the vulnerability? Financial, operational and reputational impact should be considered. Keep it simple and use the High, Medium, Low values to measure impact.

Determine Initial Risk Rating- Initial risk is defined as the risk that exists when considering how ***existing*** controls affect the likelihood and or impact of a threat being realized. For example, if you measured both likelihood and impact as low, then the initial risk rating will be low.

Determine the Risk Management Strategy – The final phase of the risk management process is determining a strategy to manage the identified risks. There are four basic strategies to reduce risks to an acceptable level.

1. Risk Mitigation – This is the most commonly used strategy and involves the implementation or enhancement of control(s) intended to reduce the likelihood or impact of the identified risk.
2. Risk Transference – This strategy involves transferring the risk to a third party (such as an insurance policy). Although this strategy does not necessarily decrease the likelihood

of vulnerability exploitation, it does lessen the impact (usually via a financial payout) to the organization.

3. Risk Acceptance – A risk acceptance strategy involves allowing a known flaw to continue to exist. If the overall impact is determined to be low, it may be more cost effective to accept this known risk rather than to implement a control.
4. Risk Avoidance – This reduces risk by discontinuing the planned change to the environment.

In light of the growing intensity and sophistication of a seemingly unlimited number of threats, an effective information security risk management program is essential. It provides the framework for a consistent and repeatable methodology to guide accurate, cost-effective resource allocation decisions for managing risks. Protecting your credit union's information assets benefits individual business units, your members and the organization as a whole.

Dean Choudhri can be contacted at dean.choudhri@alloyacorp.org. To learn more about Alloya Corporate FCU, visit www.alloyacorp.org.

**CISSP: Certified Information Systems Security Professional*