# Security Assessment Exercise

# Name: Kevin Auriemma, Amanda Krauth

Organizations are completely dependent on their IT systems. System outages can have significant operational and financial impacts on an organization. IT-Security failures may also result in unauthorized access to computer systems and the release of confidential information. Unauthorized access, and the disclosure of private information, may expose a company to significant legal liability. As IT professionals who manage these systems, we have an obligation to our stakeholders to manage the risks associated with a failure of security of our systems.

There are many techniques that can be used to manage risk. The risk management process generally consists of the following process:

1. Identify threats and exposures;

2. Implement risk controls. Risk controls are activities designed to reduce the probability of a loss, or to minimize the effects of losses that do occur (at least 1 risk control should be implemented for each exposure to loss identified)

3. Implement risk financing strategies. Risk financing activities are designed to provide funds to pay for losses that do occur. Risk financing may include the purchase of insurance, retention of risk (paying for losses using funds on hand), or contractually transferring risk to others); and,

4. Monitor changes to threats and exposures; adopt changes to risk control and risk financing techniques as appropriate.

As IT professionals we can always implement better security procedures and controls. However, often it is not practical or cost-prohibitive to adopt perfect risk controls to eliminate the risks of loss. Our challenge is to implement reasonable precautions to prevent loss based on the capabilities and business needs of the organization.

In this exercise you will work in a small team to assess the security related IT capabilities of three fictitious organizations. These fictitious organizations are:

1. West Publishing
2. Blueberry Software
3. Widgets Retail

In the first step of the risk management process, frequently companies will use questionnaires and surveys to gather information. For each organization you will be provided with a completed questionnaire. The questionnaire is based on the ISO 7799 Security Standard, and provides the responses from each organization. Each team will be assigned one of the three fictitious organizations. They will review the questionnaire for that organization and attempt to assess the capabilities of that organization. They will then review the questionnaires from the other two organizations and attempt to assess the capabilities of their organization relative to the other two organizations.

The ISO 7799 standard provides a benchmark of existing security practices against an ideal standard. The ISO 7799 standard includes nine major “domains.” Each domain consists of a critical aspect of IT-security.

Please assess the responses for each of these domains. Within each domain there may be a few questions which focus on the most critical issues. Focus additional attention on these particular questions and assess both the individual and relative capabilities of your organization in these areas.

Please complete the following table capturing your team’s assessment of the security related IT capabilities of your assigned organization. For each domain and critical issue, assign a score of high, medium, or low which represents your assessment of your organizations capabilities in these areas.

|  |  |  |
| --- | --- | --- |
| **Domain Scores** | **Individual**  **Organization**  **Capability**  **(H/M/L)** | **Relative**  **Capability**  **(H/M/L)** |
| Security Organization | **H** | **H** |
| Security Policy and Standards | **M** | **H** |
| Physical and Environmental Security | **M** | **M** |
| Computer and Network Management | **L** | **M** |
| Access Control | **H** | **H** |
| Systems Development and Maintenance | **M** | **M** |
| Compliance | **L** | **L** |
| Vendor Management | **H** | **H** |
| Business Continuity | **L** | **L** |
| **Critical Issues** | **Individual**  **Organization**  **Capability**  **(H/M/L)** | **Relative**  **Capability**  **(H/M/L)** |
| Patch management process | M | L |
| Managing user accounts | H | H |
| Virus protection | H | H |
| Access control procedures | H | H |
| Physical security controls | M | M |
| Information security policies | M | M |
| Business continuity plans | L | L |
| Information security infrastructure/ organization | H | M |
| Security configuration documentation | H | H |
| Security testing | L | M |

In addition, each team must prepare a brief (5 minute) PowerPoint presentation which highlights the most significant findings in the assessment of their assigned organization. The presentation should focus on areas where their assigned organization is doing an outstanding job. For these areas discuss what they are doing which makes them outstanding. The presentation should also focus on areas where their assigned organization is performing poorly. For these areas, provide recommendations to management on actions that can be taken to improve security. Remember perfect security is often not reasonable based on cost and other business constraints. Focus on the things the organization can do that will have the largest impact to improved security with the smallest cost or disruption to business. Yet, don’t shy away from items that are high cost or may impose significant disruptions to current business processes if these items are critical to preventing loss

The questionnaires along with the fictitious sample data that we are using in this exercise have been provided by American International Group (AIG), a world leader in the insurance and financial services industry. AIG has been a pioneer in the area of network security and liability insurance products.