Information Security Assessment

Every organization has finite resources to apply to information security. Understanding areas of risk and the organization's ability to monitor and mitigate those risks is the key to developing an appropriate risk mitigation strategy.

People looking to compromise the security of an organization look for the easiest or weakest link in the security profile of an organization. A balanced, holistic, and layered approach is required to identify and mitigate risks. Information security is an ongoing series of processes, procedures, and practices working together.

The questions facing every organization pertinent to information security are:

1. Where is the organization vulnerable?
2. How does an organization know what should be done?
3. How often should it be done?
4. What should not be done?
5. Are the resources available?
6. Does it make sense financially?

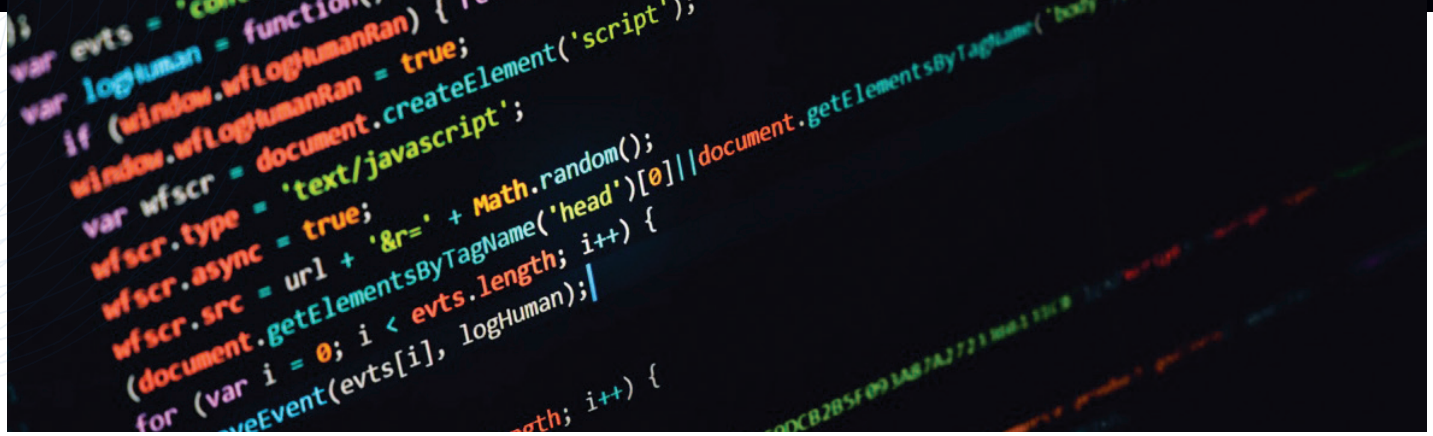
OUR APPROACH

We have developed a formal approach to helping organizations arrive at the answer to these questions and to provide a roadmap on which to proceed in their risk mitigation effort.

A custom Information Security Scorecard to aid in providing a risk assessment profile for an organization. The Information Security Scorecard was developed based on the 20+ years of experience of each of our team members dealing with security breaches and implementing preventative measures. The scorecard was designed to align with the ISO 27002:2013 framework, the internationally accepted framework for IT controls.

Structured approach to evaluating:

1. Risk tolerance level of an organization
2. Identifying acceptable risks
3. Prioritizing the activities to mitigate risks



WHAT IS ACCEPTABLE RISK?

The acceptable risk level is typically a balance of:

1. **Potential damage**
2. **Risk probability & relative priority**
3. **User inconvenience**
4. **Risk mitigation cost**

An organization has to be able to understand its risk acceptance threshold. The scorecard helps identify the risk acceptance level for each activity and documents the corresponding appropriate risk mitigation activities.

ASSESSMENT WORKSHOPS

Assessment workshops are approximately two - three hours in duration. Initial discussions outline information security risk concerns in three common categories:

1. **Major operational and revenue stream risks**
2. **Intellectual Property Risks**
3. **Brand & Reputation Risks**

The remainder of the workshop time focuses on these risk categories relative to the security scorecard controls. Our consultants will ask questions covering a series of topics including IT operations and practices, applications, and network & systems infrastructure. Maturity levels are rated from 0 to 5 and help determine how an organization compares to others for specific controls.

For each topic the following is assessed:

1. **Organizations' security maturity level and acceptable risk**
2. **Target maturity level applicable for each control**
3. **Current priority for the organization**

THE FINAL REPORT

1. Security Posture Assessment Score (CMMI Rating Scale for current & target).
2. Security Remediation Action Items based on Capacity, Budget and Risk Priority
3. Security Ecosystem Map
4. Security Remediation Roadmap (18-24 months)
5. Executive Summary & Recommendations
6. Vulnerability Assessment Report (detailed assessment results)
   - Technical Vulnerability Assessment
   - Social Engineering Vulnerability Assessment

ISO 27002 - INFORMATION SYSTEMS SECURITY AREAS IN SECURITY SCORECARD

The fourteen (14) security areas, based on the ISO 27002:2013 - Information Systems Security Framework, which will be considered are:

1. Information security policies

Þ Management responsibility for defining and supporting the IT information system security policies and procedures.

2. Organization of information security

Þ Define the roles and responsibilities for aspects of Information Systems security.

Þ Security controls for mobile devices and remote/virtual computing

3. Human resource security

Þ Security controls prior to employment, during employments, change of responsibility and terminations.

Þ Allocation and return of corporate assets, ongoing organization security education.

4. Asset management

Þ Inventory and classify information assets and define asset responsibility.

Þ Define controls for managing and controlling storage media

5. Access control

Þ Business requirements for access control, management of user's access. User responsibility towards access security. Application access control.

6. Cryptography

Þ Control of encryption use. Management of cryptographic and security keys, digital signatures.

7. Physical and environmental security

Þ Control physical access to secure areas, protection from unauthorized access, fires, floods, etc.

Þ Equipment security and protection, monitoring capability. Equipment reuse, clear desk policy

8. Operations management

Þ Operational procedures, malware protection, backups and data retention, patch management, logging and monitoring, software management

9. Communications security

Þ Network segmentation and security, policies and procedures with regards to information transfer, Mail, third party services.

10. System acquisition, development and maintenance

Þ Security controls for application systems, security with development and support, and security of test data.

11. Supplier relationships

Þ Maintaining and availability of contracts and support agreements. Security requirements and controls for third party suppliers.

12. Information security incident management

Þ Policies and procedures for reporting assessing and responding to security incidents

13. Information security aspects of business continuity management

Þ Information security continuity planning. Inform system redundancies to satisfy the organizations requirements.

14. Compliance

Þ Legal and contractual requirements, Information systems security reviews and or audits.

Other frameworks such as ITIL and COBIT have been considered and incorporated into the Scorecard.

The CMMI (Capability Maturity Model Integration) scale is used to measure the effectiveness and maturity of managing and applying security controls. The CMMI scales ranges from 0, where processes do not exist to a 5 with a well-documented continuous improvement process. Most organizations strive for the 3-4 range depending on the industry segment.

Integra Data Systems Corp.

VULNERABILITY ASSESSMENT

We use vulnerability scans where appropriate to identify potential risks. Vulnerability scans are scored on a scale of 1 to 5 with a score of 5 being the most urgent requiring immediate action.

Vulnerability Assessment scans use a combination of industry leading tools for the scans. There are two types of scans typically used:

1. **External Vulnerability Assessment (EVA)**
2. **Internal Vulnerability Assessment (IVA)**

External Vulnerability Assessment (EVA) scans your external internet-facing IP addresses for thousands of known vulnerabilities and provides easy-to-interpret reports that pinpoint your most vulnerable IPs from a ranked list. An overall rating of your security level is provided, along with a prioritized list of the vulnerabilities discovered.

Internal Vulnerability Assessment (IVA) is a powerful internal assessment of your security exposures that maps your network infrastructure from the inside and checks for known security weaknesses. IVA identifies physical and virtual devices and where appropriate tests each one for tens of thousands of known vulnerabilities. Internal vulnerabilities are those weaknesses that could be exploited by a malicious employee, a contractor, or an attacker that has gained access to your internal network.

SEVERITY CODE	SEVERITY LEVEL	DESCRIPTION
1	Minimal	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
2	Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
3	Serious	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
4	Critical	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
5	Urgent	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Integra Data Systems Corp.