for ***Some Good Organization***

YOUR NEEDS ASSESSMENT REPORT

Contents

Introduction 3

Overview of Results 4

Information Security Fundamentals 5

Detailed Risk Analysis 7

Focus Area 01 – Risk Assessment 8

Focus Area 02 – Information Security Policy 9

Focus Area 03 – Program Management and Support 10

Focus Area 04 - Asset Management 11

Focus Area 05 - Trustworthy Human Resources 12

Focus Area 06 - Physical and Environmental Security 13

Focus Area 07 Information Technology Communications and Operations 14

Focus Area 08 - Access Control 16

Focus Area 09 - Systems and Application Development 17

Focus Area 10 - Incident Response 18

Focus Area 11 - Business Continuity Management 19

Focus Area 12 - Program Maintenance and Compliance 20

Compliance (sample only) 21
Gramm-Leach-Bliley Act 21

Next Steps 22

Introduction

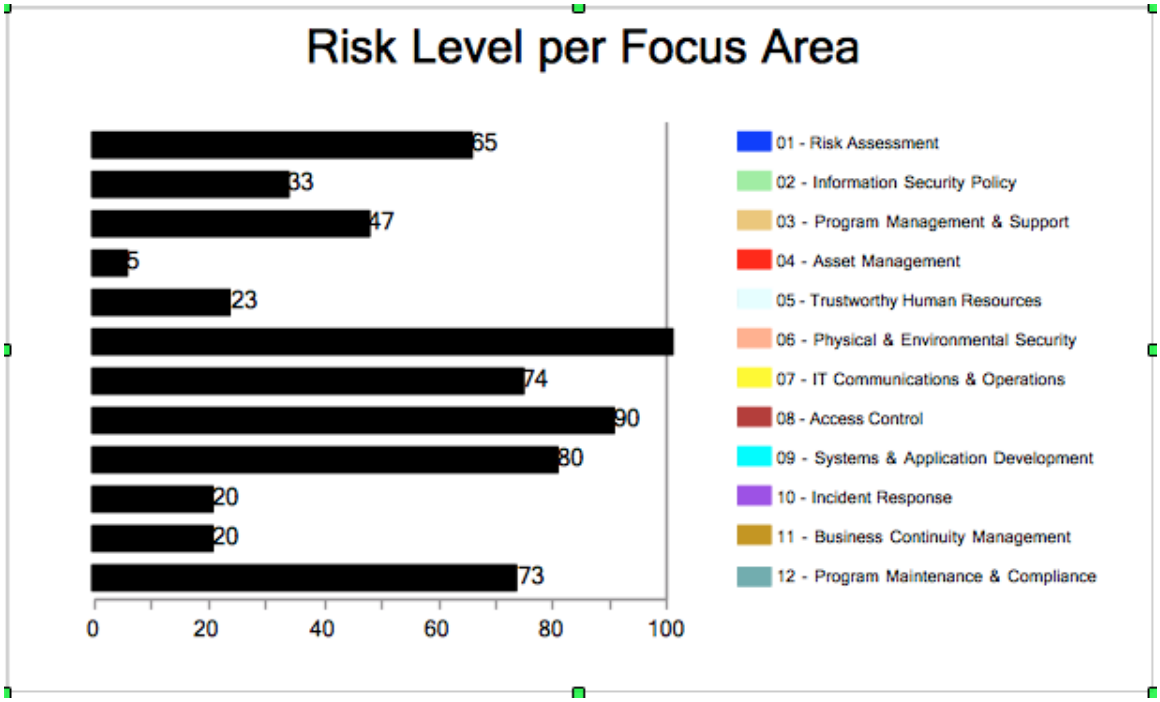
Thank you for taking the time to complete this Needs Assessment Survey. We look forward to helping you understand your own unique strengths and needs. Over the next few pages we will examine your answers in relation to how they contribute to your overall threat profile. This report will help you understand what risks your business face, and make suggestions for improving your Information Security Program.

Many organizations report feeling a bit overwhelmed after reading this report. This is normal when you are starting to build your Information Security Program. Rest assured that you are not alone in this feeling, and that it is easy to overcome it once you get started in addressing your particular needs especially when you have someone to guide you through the process.

It should be noted that this Needs Assessment should not be substituted for a full risk assessment. For this assessment, we are relying solely on information you have provided us, and have not done anything further to verify this data.

Finally, we welcome the opportunity to discuss this report with you. We know that sometimes starting down the path to securing your information seems fraught with obstacles. We have helped thousands of clients secure their information. And, we will be happy to help you get started in securing yours.

Overview of Results



Overall Risk Level: Medium

Overall Risk Score: 61%

Information Security Fundamentals

Information Security can seem very complex. For most organizations however, there are some fundamental items that when implemented correctly will cover most of your Information Security needs. Every organization, regardless of size or complexity needs to have these items in place. Because of this necessity, *Net Reaction* uses this as a starting place for assessment. As a practical take away, if you find yourself deficient in these fundamentals, you need to start here before focusing elsewhere.

	Area	*Your Rating*
Assessment	Risk Assessment • Risk Assessment is the critical tool for understanding the threats to your organization. You cant protect what you dont understand. Risk Assessment is the first step that any organization should take in developing an Information Security Program.	Deficient
Policies & Procedures	Information Security Policy • Describes what information needs to be protected and why, expresses managements commitment to protecting the information and describes to the reader how the information is to be protected.	Deficient
	Acceptable Use Policy • Describes what actions the reader may and may not take in working with and handling the organizations information	Passing
	Employee Handbook • Expresses the organizations expectations of the reader as conditions of their employment	Passing
	Background Screening Policy • Gives the organization the employees permission to conduct appropriate background checks as a condition of their employment	Deficient
	Confidentiality Policy • Explicitly states to the reader that all information encountered during their employment is the property of the organization	Deficient

	Area	*Your Rating*
Technical Controls	Firewall Policy • Firewalls are necessary for anyone storing sensitive information on their corporate networks	Passing
	Wireless Policy • Wireless networks should be appropriately secured on networks where sensitive information is present	Deficient
	Password Policy • The selection of appropriately strong passwords is one of the most fundamental, yet effective information security controls	Passing
	Data Classification • Data should be classified according to sensitivity and protected accordingly	Passing
	Remote Access • When used, remote access points need to be appropriately configured and secured	Passing
	Secure Disposal of Information • Information and media must be appropriately destroyed before disposal or reuse	Passing
Other Controls	Vendor Integrity Assessment • The vendors and third parties you work with are critical in the protection of your information. Your security doesnt matter if they dont have appropriate controls in place.	Passing
	Incident Response Plan • Incidents happen to even the most prepared organizations. An incident response plan is critical in minimizing the damage to your organization	Deficient
	Employee Training • You cant do what you dont know. Your organization must communicate its expectations to your employees through training.	Passing

Detailed Risk Analysis

The following sections will analyze your strengths and needs in each of the focus areas of Information Security. Each focus area is important and contributes to the overall effectiveness of your Information Security program. Focusing too much on one area while neglecting another area can leave your organization vulnerable to information crimes.

It should be noted that this Needs Assessment is meant to give the user a quick snapshot of their Information Security Program, and is not intended to replace a full enterprise risk assessment by a certified auditor.

Focus Area 01 – Risk Assessment

Risk assessment is the foundation of information security planning. If your organizations Information Security Program is going to be effective, the program must address the unique risks faced by your organization. Risks must be fully identified and understood before effective mitigation strategies can be developed. Risk assessment addresses both the process of identifying vulnerabilities and threats as well as the probabilities of their occurrence and potential impact.

Your Information Security Program should include at least the following:

- ☐ A framework for the identification and quantification of risks to your organization
- ☐ A strategy for developing mitigation strategies to address risks to your organization
- ☐ Periodic review and update of your risk assessment

Risk Level: Medium
Your Score: 65%
Recommendations:

- Consider formalizing your risk assessment framework.

Focus Area 02 – Information Security Policy

Documentation of policy is imperative in outlining the principles of any Information Security Program. These policies address management directives for establishing information security for the organization, identify relevant contracts, laws and regulations constraining the organization, and sets procedures to be used in day-to-day operations.

An effective set of Information Security policies should include at least the following:

- ☐ Establishment of an Information Security Policy
- ☐ Establishment of an Employee Handbook
- ☐ Establishment of a Review Schedule for appropriate policies

Risk Level:	High
Your Score:	33%

Focus Area 03 – Program Management and Support

All information security responsibilities should be defined for employees and addressed appropriately with external parties. An effective Information Security Program requires a supporting structure within the organization as well as necessary controls for customers, contractors, or partners to sustain a successful information security program.

Your Information Security Program should include at least the following:

- ☐ To organize the support structures for an effective information security program
- ☐ Ensuring managements support for information security
- ☐ Coordination of information security roles and the allocation of responsibilities among staff
- ☐ Establishment of authorization processes
- ☐ Establishment of Non-Disclosure policies and confidentiality agreements
- ☐ Establishment of relationships with external parties and special interest groups
- ☐ Management of external relationships

Risk Level: High

Your Score: 47%

Recommendations:

- Formalize your individual pieces of a program into a formal Information Security Program — Consider implementing a formal update schedule for your organizational policies — Consider having an outside third party review your organization's Information Security posture on a periodic basis — The methods that vendors and third parties use to protect your data are as important as the method and controls you use. Assess your vendors' Information Security programs before conducting business — Consider making the protection of your organization's information a part of your vendor contracts

---

Focus Area 04 - Asset Management

Just like risk assessment, you cant protect something if you dont know you have it. As an essential part of risk management and disaster recovery, an inventory of assets and information should be maintained by the organization. Without it, the organization has no idea what it is protecting. An effective program should contain guidelines for data owners, classification guidelines, labeling and handling guidelines and establish the acceptable use of information.

Your Information Security Program should include at least the following:

- ☐ Establish an asset inventory
- ☐ Implementation of classification guidelines
- ☐ Identifying owners for the organizations information and assets
- ☐ Establishing Information Labeling and Handling Policies
- ☐ Establishing an Acceptable Use Policy

Risk Level: High
Your Score: 5%
Recommendations:

- Consider formalizing your Data Classification Guidelines — Organizational assets and information should be clearly labeled and identified according to your Data Classification Guidelines

---

Focus Area 05 - Trustworthy Human Resources

Protection of information cannot be expected by default. Employees, contractors, vendors and other related third parties each have obligations to protect your organizations information. Beginning with trustworthy personnel, the organization should offer training for defined information security expectations and have a disciplinary plan for handling information security incidents.

Your Information Security Program should include at least the following human resource concerns:

- ☐ Documentation of roles and responsibilities
- ☐ Establishment of a background screening policy
- ☐ Review of Terms and Conditions of employment
- ☐ Implementation of Information Security Awareness, Education and Training
- ☐ Establishment of formal disciplinary and termination processes

---

Risk Level: ¡¡Area5RiskLevel¿¿
Your Score: ¡¡Area5Score¿¿%
Recommendations:

- ¡¡Area5Recommendations¿¿

Focus Area 06 - Physical and Environmental Security

Proper concern should be given to physical and environmental threats that are either natural or man-made. Everything from the physical perimeter, placement of equipment storing sensitive information and contingency plans for environmental disasters must be assessed. This section highlights characteristics to consider for protecting the organizations information security from such issues.

Your Information Security Program should include at least the following:

- ☐ Assessment of the physical security perimeter
- ☐ Evaluation of physical entry controls, office security, external and environmental threats, public areas and loading docks, supporting utilities and cabling
- ☐ Assessment of equipment security located offsite
- ☐ Establishment of Information Disposal and Reuse policies
- ☐ Controlling the removal of property

Risk Level: ¡¡Area6RiskLevel¿¿

Your Score: ¡¡Area6Score¿¿%

Recommendations:

- ¡¡Area6Recommendations¿¿

Focus Area 07 Information Technology Communications and Operations

Todays business environment relies on networked computer systems to retain, process, and produce immense amounts of information. Attention needs to be given to ensuring that these assets protect your organizations information as opposed to creating a liability. Appropriately secure systems need to be properly configured, have documented operating procedures and audit trails.

Your Information Security Program should include at least the following:

- Evaluation of operating procedures
- Establishment of operating policies including change control, segregation of duties, separation of production systems, capacity management, system acceptance, malicious code, mobile code, information backup and media disposal
- Review of network controls, electronic messaging, ecommerce, interconnections of business information systems and online transactions
- Establishment of audit logging and the protection of log files

Risk Level: Medium
Your Score: 74%
Recommendations:

- Careless disposal of information is a leading cause of data breaches. Make sure that all media and information is securely destroyed before disposal or reuse — Consider setting your antivirus solution to update and run at least once per week on your workstations. — Consider implementing formal change control procedures to evaluate and if necessary roll back changes made to the organization's systems. — Consider archiving audit logs for all user activity as appropriate. Audit logs make both troubleshooting and investigations easier and less time consuming. — Assign someone to review your audit logs on a periodic basis. Many instances of fraud have been uncovered by a casual glance at log files. — Test your backup media from time to time, especially if you are using cassette media. Backup media has a finite lifespan and must be replaced periodically. — Consider whether you really need sensitive personal information to be stored on laptop computers. In cases where the answer is yes, continue with whole disk encryption. — Consider whether or not business applications really require sensitive personal information to be collected via the web. In cases where the answer is yes, ensure that you continue the use of appropriate encryption. — Consider formally testing your websites for common vulnerabilities on a periodic basis. — Consider whether or not your business really needs to store credit card information. In cases where the answer is yes, continue the use of appropriate encryption.

Focus Area 08 - Access Control

Access to the organizations information should be restricted based on classifications and the requirements of the Information Security Policy. This section examines this integral issue from general policy to the specifics of password selection and timeout controls.

Your Information Security Program should include at least the following:

- Establishment of access controls
- Management of user registration and access privileges
- Protection of unattended equipment
- Controlling use of network services through authentication, equipment identification, secure logon procedures, session timeouts and limited connection times
- Protection of network equipment through disabling remote management ports
- Segregation of networks
- Sensitive system isolation
- Controls for employees who work remotely

Risk Level: tbd
Your Score: 0%
Recommendations:

- tbd

Focus Area 09 - Systems and Application Development

Systems and application development is an area where Information Security needs are often overlooked. The perceived need to get systems up and running quickly sometimes supersedes the need to consider security requirements. Controls are needed for information technology systems to ensure confidentiality, integrity and non-repudiation of your organizations sensitive information. This section reviews the protection and verification procedures needed for all systems and applications.

Your Information Security Program should include at least the following:

- Specification of security requirements for applications and systems
- Validation of input and output data
- Establishment of a cryptographic control policy
- Protection of system test data, program source code and operational software
- Prevention of information leakage
- Control of outsourced software development
- Properly addressing technical vulnerabilities and updates

Risk Level: tbd
Your Score: tbd%
Recommendations:

- tbd

Focus Area 10 - Incident Response

Incidents happen, even to the best organizations. Organizations that are prepared to respond when incidents occur respond faster, with fewer financial losses and with less damage to their brand integrity and reputation. Formal procedures should be established for handling information security events. This section covers the basics needed regarding incidents from prevention to lessons learned.

Your Information Security Program should include at least the following:

- Establishment of procedures for reporting information security events and security weaknesses
- Establishment of incident response procedures
- Ensuring that evidence is collected properly
- Ensuring that lessons are learned from information security incidents

---

Risk Level: ¡¡Area10RiskLevel¿¿

Your Score: ¡¡Area10Score¿¿%

Recommendations:

- ¡¡Area10Recommendations¿¿

Focus Area 11 - Business Continuity Management

Planning for business continuity in the event of any disruption is vital to an organization. While most organizations have an existing framework for handling business interruptions, this section addresses specifically including and maintaining information security into that process.

Your Information Security Program should include at least the following:

- Inclusion of information security in the business continuity planning process
- Establishment of a common business continuity framework
- Implementation of business continuity plans
- Testing, maintaining, and regular reassessment of the business continuity plans

---

Risk Level: ¡¡Area11RiskLevel¿¿

Your Score: ¡¡Area11Score¿¿%

Recommendations:

- ¡¡Area11Recommendations¿¿

Focus Area 12 - Program Maintenance and Compliance

Once an Information Security Policy Program is established, ensuring it remains relevant is essential. This section describes necessary maintenance of the program including legal requirements, upgraded standards and audit considerations.

Your Information Security Program should include at least the following:

- Identification of applicable legislation and regulatory requirements
- Recognition of intellectual property rights
- Protection of organizational records
- Protection of Personally Identifiable Information and Non-Public Information
- Compliance with cryptographic regulations
- Establishment of audit procedures for information systems and the protection of system audit tools

---

Risk Level: ¡¡Area12RiskLevel¿¿

Your Score: ¡¡Area12Score¿¿%

Recommendations:

- ¡¡Area12Recommendations¿¿

Compliance (sample only)

Gramm-Leach-Bliley Act

Compliance Requirement: Required

The Financial Services Modernization Act of 1999, better known as the Gramm-Leach-Bliley Act repealed part of the Glass-Steagall Act of 1933. This law provided an opening for investment banks, commercial banks, securities firms and insurance companies to consolidate. From an Information Security perspective, two key rules under the Act make it significant. First the Financial Privacy Rule puts restrictions in place governing the collection and distribution of a customers personal financial information. This applies to both financial institutions, creditors and any company that receives such information. Second, the Safeguards Rule requires that affected organizations much design, implement and maintain appropriate safeguards to protect customer information. The Safeguards rule applies to both financial institutions that collect information from their customers, but also to institutions that receive customer information from other institutions.

Requirements:

Financial Privacy Rule

1. Provide each customer with a privacy notice at the time a consumer relationship is established
2. Provide a privacy notice to each customer on an annual basis
3. Establish a means by which the consumer may opt out of their information being shared with unaffiliated parties
4. Notify consumers anytime there is a change to the privacy policy

Safeguards Rule

1. Assign an employee to oversee the safeguards
2. Perform a thorough risk assessment on any business operation that handles nonpublic information
3. Develop a program, monitor and test the program to secure information
4. Update the program as necessary as changes are made to how information is collected, stored or used

Next Steps

What should I do next? Our key recommendations are prioritized for you here:

- Stop to smell the roses. — Call your mother. — Do the next thing on your bucket list.

Thank you again for taking the time to complete this Needs Assessment.

If you are like most of the organizations that we work with, youve just finished reading this report and have some major questions about where to go from here. Rest assured that *Net Reaction* has helped thousands of organizations understand their Information Security Needs, and is committed to helping you understand your organizations specific needs.

Every organization is different, and each has areas in which they can improve. We have highlighted some of those areas for your organization in this report. We would be happy to discuss them with you further, and invite you to give us a call at your convenience to speak about your path forward from here.

Sincerely,

Bryan Thornton
bthornton@net.reaction
1-888-211-1644
9-5 PDT ()UTC-7)
Net Reaction, LLC