

## Survey Quick eRisk Assessment

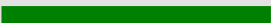







Survey's scorecard  
Quick eRisk Assessment

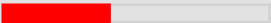




This is a eRisk Hub sponsored 'fast self-assessment', designed to capture high-level information concerning your company's use of some industry-recognized baseline practices in the areas of IT security.

This eRisk Hub fast self-assessment is based upon a very limited survey (sampling) of network risk factors and industry recognized baseline practices associated with network security and related processes. By offering this NetDiligence nor our alliance partners make any representations about the actual or potential risk exposures associated with the customer, nor do we certify any form of security state or compliance.




## Report Card Calculation Methodology

This report card is intended to highlight your organizations' overall score on the Self-Assessment. The total possible score is 100. This report card may indicate areas of improvement for your Network Security and Risk Management Program. For specifics on which areas or questions you scored high and low on, please review the survey and your answers. Negative or 'no' responses will indicate the areas for your improvement.




Section	Summary	Scores	Issues
1 Security Policy A written policy document should be available to all employees responsible for information security.	Ok	Your score 100% 	N/A
2 Security Organization To manage information security within the organization, a management framework should be established to initiate and control the implementation of information security within the organization	Weak	Your score 50% 	N/A
3 Information Asset Classification and Control To maintain appropriate protection of organizational assets and, to ensure that information assets receive an appropriate level of protection.	Ok	Your score 100% 	N/A
4 Personnel Security To reduce the risks of human error, theft, fraud or misuse of facilities. To ensure that users are aware of information security threats and concerns, and are equipped to support organizational security policy in the course of their normal work.	Weak	Your score 50% 	N/A
5 Physical and Environmental Security To prevent unauthorized access, damage and interference to IT services. To prevent loss, damage or compromise of assets and interruption to business activities.	Ok	Your score 100% 	N/A
6 Communications and Operations Management To ensure the correct and secure operation of computer and network facilities. To minimize the risk of systems failure. To safeguard the integrity of software and data. To maintain the integrity and availability of IT services.	Ok	Your score 66% 	N/A
7 Access Control To control access to business information. To prevent unauthorized computer access. To prevent unauthorized user access. Protection of networked services. To prevent unauthorized access to information held in computer systems. To detect unauthorized activities.	Ok	Your score 100% 	N/A
8 Systems Development and Maintenance To ensure that security is built into IT systems. To ensure that IT projects and support activities are conducted in a secure manner. To maintain the security of application	Weak	Your score 50% 	N/A

	Section	Summary	Scores		Issues
	system software and data.				
9	Business Continuity Management To have plans available to counteract interruptions to business activities, resulting from network attacks or outages.	Weak	Your score	40% 	N/A
10	Compliance Compliance with legal requirements, to mitigate breaches of any statutory, criminal or civil obligations and of any security requirements. To ensure compliance of systems with organizational security policies and standards.	Ok	Your score	75% 	N/A
11	Data Privacy Practices To ensure that there is general awareness of privacy issues surrounding data and information management, based on recognized Fair Information Principals including - Privacy policy Notice and Awareness; Customer Choice and Consent; Customer access; Privacy policy enforcement and accountability.	Ok	Your score	100% 	N/A
12	General & Current Events To capture a high level understanding of what your organization is doing to pro-actively address a few 'current event issues' confronting businesses with security and/or liability implications attached to same.	Ok	Your score	100% 	N/A
Score Average and Total Issue Sections			Your score	77.6% 	

Summary terminology

	OK	The responses to the applicable questions in the survey indicate that most or all of the best practices are observed. Where 'OK' appears with a green light, the company achieved 65% or more of the applicable points within a given section.
	OK	The responses to the applicable questions in the survey indicate that most or all of the best practices are observed. Where 'OK' appears with a yellow light indicates the company achieved a marginal passing score between 55-64%.
	Weak	The responses to the applicable questions in the survey indicate that best practices are not being followed and that significant vulnerabilities may exist. The company achieved less than 55% of the applicable points for a given section.

Issue terminology

	N/A	No issues-based questions have been designated in this section that reflect critical requirements or address a baseline control.
	Issue	The responses to the applicable questions in the survey indicate that while best practices are observed in some or most cases, inattention to certain critical requirements exist and immediate attention toward these items may be necessary. Regardless of the score achieved by the company for a given section, responses to one or more key questions indicated a specific weakness that must be addressed immediately.
	No issue	No issues have been found.

## Survey Quick eRisk Assessment

This assignment was sent to Success Sciences.

### Full Questionnaire

---

#### 1) Security Policy

**1.1) Does your company have a current enterprise-wide computer network and information security policy that applies to all employees, independent contractors and third-party vendors?**

Yes

(Best practice: A formal policy informing employees and contractors of their obligation to perform information security tasks as part of their ongoing job duties is essential. It should be drafted and implemented through senior management and the IT security function.)

**1.2) Have you published the information security policy within the company (via the corporate Intranet, employee handbooks, etc.)?**

Yes

(Best practice: If information security policies are not publicized, the company cannot reasonably expect uniform adherence to them by every employee. Even well-meaning employees may not be aware of the technology-based requirements that may be included in the company's procedures. Moreover, this may help to meet any legal requirements about notice and assent.)

#### 2) Security Organization

**2.1) Is there a departmental function within the company that is staffed with dedicated (or "dotted-line") information security employees who assist the information security manager in carrying out compliance operations?**

N/A

(Best practice: This may or may not be applicable depending on the size of your company. Companies with significant assets and/or complex network operations usually need a dedicated team to properly maintain a secure network environment. Moreover, security functions can overwhelm a CIO or IT manager who is primarily concerned with maintaining network operations.)

**2.2) If the company maintains dedicated network connectivity with - or outsources mission-critical IT functions to - third-party clients/vendors, are there adequate contractual provisions and sufficient functional controls in place to enforce your information security policy and procedures?**

Yes

(Best practice: Without legally enforceable security language in outsourcing contracts (SLAs), the company has little recourse in the event of a network security breach caused by negligence on the part of a vendor. Many vendors view network security protection as a 'service feature' that must be purchased separately from the primary business service.)

### 3) Information Asset Classification and Control

**3.1) Is there an information classification program that specifies different levels of security based on the business-critical nature of a given information asset?**

Yes

(Best practice: A sophisticated information security program specifically identifies sensitive information to ensure that it is handled and secured properly. The program also should assist with cost justification budgets for implementing safeguards.)

**3.2) Has your organization implemented effective procedures for appropriate labeling and handling of information assets that are associated with your most sensitive classification levels?**

Yes

(Best practice: Appropriate classification of an organization's most sensitive information assets must be supported through functional procedures that ensure employee compliance with the organization's protection efforts.)

### 4) Personnel Security

**4.1) Are formal background checks conducted on all prospective new hires in order to identify the existence of criminal records, proof of educational attainment, and acceptable performance in past employment?**

No

(Best practice: Conducting background checks on potential employees can help mitigate the potential for insider fraud and abuse.)

**4.2) Are all employees periodically instructed on their specific job responsibilities with respect to information security, such as the proper reporting of suspected security incidents and other "due care" tasks?**

Yes

(Best practice: Unless employees are encouraged to report potential incidents and informed about how to report a suspected breach, the IT staff may not be able to respond in the most timely manner.)

### 5) Physical and Environmental Security

**5.1) Does the company maintain a physical security perimeter around all IT processing facilities, and is it designed using significant barriers to minimize the opportunity for unauthorized entry?**

Yes

(Best practice: As direct access to network equipment is a relatively easy way to compromise or destroy sensitive information, only authorized employees should have access to the rooms housing IT processing facilities.)

**5.2) Has a risk assessment been performed on all IT processing facilities to take into account the probabilities of extraordinary events (earthquake, flood, attack, etc.), and have company managers taken reasonable steps to mitigate these risks?**

Yes

(Best practice: A formal risk assessment is an important step in prioritizing funding, personnel, and security-based focus on those assets and activities deemed to be mission-critical to the organization.)

## **6) Communications and Operations Management**

**6.1) Is all sensitive non-public customer information encrypted when it is transmitted over external networks AND within local database or file in storage?**

N/A

(Best practice: Any financial or other personally identifiable information should be encrypted before transmission via the public Internet, preferably under a 128-bit or higher standard.)

**6.2) Are system backup and recovery procedures documented/tested for all mission critical systems and performed at least once per week?**

Yes

(Best practice: Unless the company regularly tests backup and recovery capabilities to ensure that 'live' events go smoothly, unanticipated problems may appear at the worst possible time. Properly backing up data is critical to business continuity and disaster recovery planning. For high volume and high-availability networks, backups should be scheduled daily or even continuously.)

**6.3) Are anti-virus procedures used on Internet-facing and internal mail servers, desktops and other mission-critical servers?**

Yes

(Best practice: Viruses are constantly introduced to networks via e-mail and the downloading of files by employees. AV technology should be pushed down to the desktop level in all environments.)

## **7) Access Control**

**7.1) Are documented procedures in place for user account registration, assignment of access rights, password management, and routine review by business/IT managers to ensure up-to-date status and accuracy?**

Yes

(Best practice: Documented procedures that address the access rights of individual account owners must be enforced on a continuing basis to ensure that the organization retains effective control over its computing resources.)

**7.2) Are all passwords on mission-critical systems required to be non-trivial, at least six characters in length, and changed on a periodic basis?**

Yes

(Best practice: Poorly chosen (dictionary-based) passwords are one of the leading causes of a security breach and are a major vulnerability. 'Password cracking' software is prevalent and is highly efficient and effective. Ideally, password authentication should be augmented by physical 'token' devices that require a user to type in a random number generated from a keychain-sized device that remains with the individual.)

## **8) Systems Development and Maintenance**

**8.1) Does your application development process (or those of your third-party vendor-developers) make use of multi-stage, code promotion procedures in order to segregate development from production facilities?**

Yes

(Best practice: Multi-stage code development is a primary requirement in modern application development practice, and must be managed effectively in order to minimize the likelihood of unanticipated flaws appearing in production-ready applications.)

**8.2) Have authentication and non-repudiation controls been integrated into transaction-based applications?**

N/A

(Best practice: Transaction-based applications must provide independent and objective means for ensuring the authenticity of an employee's or customer's actions in order to provide legally-sufficient evidence later on if required for legal proceedings or other sensitive business events.)

## **9) Business Continuity Management**

**9.1) Are there fault tolerant or redundant components that control access to the company's trusted systems to and from all external networks (e.g. firewalls, routers, Web server hot sites, application servers, etc.)?**

Yes

(Best practice: The failure of security hardware/software can leave a network wide open to attack and abuse. The use of redundant equipment such as a Web servers and firewall appliances should be included in any business continuity planning exercises.)

## **10) Compliance**

**10.1) Are mission-critical transaction and security logs reviewed periodically for suspicious activities?**

N/A

(Best practice: Reviewing security logs on a regular basis allows IT administrators to identify potential instances of attempted 'hacking,' fraud or other abuse so vulnerabilities are mitigated and corrective action can be taken. You will be amazed at the results and amount of attempts uncovered during the review.)

**10.2) Are regular security reviews of IT systems conducted by internal audit personnel, and on at least an annual basis by a trusted third party?**

Yes

(Best practice: An ongoing review and audit process is necessary to ensure compliance with best practices and the written security policy, and to identify any new vulnerabilities that may surface. In many cases, this is best accomplished by professionals who can bring more objectivity to the exercise.)

**10.3) Has your company undergone a recent comprehensive penetration test to verify the security of all perimeter network controls (e.g. firewalls, external routers, remote access servers, etc.)?**

Yes

(Best practice: Running commercially available scanning and penetration tools against key network components can help identify any weaknesses in a company's security stance which require correction. Penetration testing will challenge your machines by simulating known 'hacker' attacks and system vulnerabilities which, if left unchecked, will ultimately lead to the vast majority of system compromises.)

**10.4) Are there incident management procedures and technologies (such as an intrusion detection system) in place to respond to suspected intrusions detected on any components that control access to the company's trusted systems to and from all external networks (e.g. firewalls, routers, Web servers, application servers, etc.)?**

Yes

(Best practice: Network attacks and/or system breaches are inevitable over time. Good security needs to be complemented by a good response plan. Together, they can effectively mitigate potential damages. Proper security planning must include a framework for action once a breach is identified. All users must also be advised who to contact in the event of a suspected intrusion.)

## **11) Data Privacy Practices**

**11.1) Does your company have a formal privacy policy that has been approved by legal counsel?**

Yes

(Best practice: This is a baseline standard. Formal privacy policies governing the use of personally identifiable information and sensitive data should be in place if you maintain data of this nature on your systems. Properly crafted and managed privacy policies are required by law in the financial services industry and other settings.)

**11.2) Are your information systems and supporting business procedures prepared to honor customer preferences concerning the opt-out of sharing of nonpublic personal information to non-affiliated third parties?**

Yes

(Best practice: Internal policies and procedures governing the use of sensitive information must be consistent with the company's privacy policy. This is especially important in the area of marketing alliances and initiatives with other companies.)

## 12) General & Current Events

**12.1) Do you require the transmission of personal customer information (such as credit card numbers, contact info, and/or product preferences) as part of your Internet-based Web services?**

No

**12.2) During the past year, has your company experienced any serious information security incidents, breaches, successful virus attacks, resulting in significant losses of data or money, potential legal liability, or significant damage to the company's overall reputation?**

No

**12.3) Does your company stay abreast of the latest federal and state laws that may require certain security standards or procedures, such as those needed in the event of a network security event/ breach (e.g. California's SB 1386 customer notification law following a breach)?**

Yes

**12.4) Does your IT department (or outsourced 3rd party vendors/providers) keep up with patches and upgrades to mission-critical systems, including all firewalls, Web servers, and Internet-accessible network components?**

Yes

(Best practice: A solid patch management process that includes system hardening measures is arguably the number one way to defeat the majority of cyber threats. This also mitigates potential legal liability exposures, which may result from a network breach.)