Thank you for interest in the NetDiligence® Expanded eRisk Self-Assessment.

When you click on the link for the Expanded eRisk Self-Assessment, you will be asked to register for the assessment by providing your organization's name, your name and your email address.

Once you've submitted your registration, you'll see an invitation to take the survey. We will also send you an email version of the invitation. You can access the survey from either the online invitation or the email invitation. This allows you to access the survey multiple times as needed to complete different sections. Once you have completed the entire survey, simply click the "Submit" button to generate your scorecard. You will be able to print the scorecard and your responses for your records.

Please be aware that this assessment will provide you with a high-level view of your cyber risk strengths and weaknesses. For a more in-depth view, consider engaging NetDiligence to perform an independent, third-party assessment. After successfully completing this free survey, ***you will be eligible for a significant discount*** on any of NetDiligence's comprehensive insurability assessments. For additional details, please contact us at management@netdiligence.com.

SEE SAMPLE SCORECARD ON NEXT PAGE.

The Expanded eRisk Self-Assessment is available exclusively through the eRisk Hub®.

Cyber Risk Assessment & Data Breach Services

eRisk Assessment by NetDiligence

SCORE CARD

Print this Page

Expanded eRisk Self-Assessment for eRisk Hub Clients

Back to Dashboard

Company Name: NetDiligence
Invitation sent to: Dave Chatfield
Submitted: 2012-11-02 00:00:00.0

This report scores the company in distinct e-risk categories based on responses provided for the NetDiligence Online survey. Please see the scoring legend below to interpret the results shown on this page. If approved by the party ordering your assessment, you will be able to view a complete list questions and your responses (including text-based) in the dashboard.

Disclaimer:

This Expanded eRisk Self-Assessment is based upon a limited (sampling) survey of network risk factors and industry recognized 'best' and baseline practices associated with information and network security and related processes. By offering this service, NetDiligence does NOT make any representations about the actual or potential risk exposures associated with the customer.

Calculation: **Report Card Calculation Methodology**

This report card is intended to highlight your organizations' overall score on the Expanded eRisk 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.

	Summary	Score	Issue	Comparison To Others
Security Policy Description A written policy document should be available to all employees responsible for information security.	OK	77.5%	✔	77.5%
	Your Score: 77.5% Comparison To Others: 77.5%			
Security Organization Description 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	OK	67.5%	✔	67.5%
	Your Score: 67.5% Comparison To Others: 67.5%			
Information Asset Classification and Control Description To maintain appropriate protection of organizational assets and, to ensure that information assets receive an appropriate level of protection.	OK	80.0%	✔	80%
	Your Score: 80.0% Comparison To Others: 80%			
Personnel Security Description 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.	OK	90.0%	✔	90%
	Your Score: 90.0% Comparison To Others: 90%			
Physical and Environmental Security Description To prevent unauthorized access, damage and interference to IT services. To prevent loss, damage or compromise of assets and interruption to business activities.	OK	72.5%	✔	72.5%
	Your Score: 72.5% Comparison To Others: 72.5%			
Communications and Operations Management Description 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	70.5%	✘	70.5%
	Your Score: 70.5% Comparison To Others: 70.5%			
Access Control Description 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	85.0%	✔	85%
	Your Score: 85.0% Comparison To Others: 85%			
Systems Development and Maintenance Description 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 system software and data.	OK	74.0%	✔	74%
	Your Score: 74.0% Comparison To Others: 74%			
Business Continuity Management Description To have plans available to counteract interruptions to business activities, resulting from network attacks or outages.	OK	64.5%	✔	64.5%
	Your Score: 64.5% Comparison To Others: 64.5%			
Compliance Description 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	76.0%	✔	76%
	Your Score: 76.0% Comparison To Others: 76%			
Privacy Description 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	70.5%	✔	70.5%
	Your Score: 70.5% Comparison To Others: 70.5%			
Score Average and Total Issue Sections	OK	75%	1	75%

Your Score: 75%
Comparison To Others: 75%

Back to Dashboard

Scorecard Extension

Baseline Safeguard Controls & Practices (at-a-glance)	
1. Internet firewall in place and properly managed	Yes
2. Anti-virus software in place and kept updated	Partial
3. Firewall log management exists	Partial
4. System backups performed on regular basis	Yes
5. Sensitive data encrypted over public networks	No
6. Redundancy of mission-critical systems	No
7. Functioning change management process[TAB]	Yes
8. Effective user account/password management	Partial
9. Tested disaster recovery plans in place	Partial
10. Legal review of Internet-based intellectual property	No
11. Effective privacy policy and aligned IT procedures	No

Summary Terminology

OK (green)	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 (yellow)	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.
✔ Issue	No issues have been found.

Final percentages in each section are based on point values assigned to questions requiring a **Yes/No/NA** response. Several questions throughout the survey have been designated as critical. If any of these are answered incorrectly, an Issue result appears for the applicable section indicating that a significant vulnerability may be present. Text-based questions have no point values, and the responses to these questions are noted by NetDiligence security engineers for subsequent discussions and/or are included in any written reports that are produced.

You may return to this page at any time by clicking the 'Score card' button in the dashboard.