

**Company name:** eRisk Hub  
**Invitation sent to:** Organization  
**Submitted on:** 07/28/2016 00:00 AM

## Expanded eRisk Self-Assessment for eRisk Hub Clients

The assessment is designed to capture high-level information concerning your company's use of industry-recognized best practices in the areas of - IT security, privacy, and intellectual asset management. Questions are based, in part, on ISO 17799 standards, with a focus on such topics as network security, the management of sensitive information, business continuity planning, and privacy.

NetDiligence conducts cyber risk assessments for organizational clients of all sizes and industry segments. As an eRisk Hub client who completes our Expanded eRisk Self-Assessment, you are eligible for preferred pricing options on our range of formal risk assessment offerings. Within the scope of these offerings, we can utilize the results of your completed Expanded eRisk Self-Assessment survey and further streamline the process for producing an industry-leading deliverable report for use in directing your Information Security/Privacy teams toward future improvements -or in applying for (or renewing) your cyber risk insurance policy. For more details, contact us today at [management@netdiligence.com](mailto:management@netdiligence.com) and learn how we can help!

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.

### Upgrade to a Formal Assessment!

Once you have completed this Expanded eRisk Self-Assessment, you will be eligible for **preferred pricing** on a NetDiligence® Cyber Risk Assessment. Our enterprise-wide Cyber Risk Assessments give you a 360 degree view of your people, processes and technology, so you can:

- **Reaffirm** that reasonable practices are in place
- **Harden** and improve your security
- **Qualify** for network liability and privacy insurance
- **Bolster your defense posture** in the event of class action lawsuits

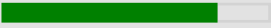

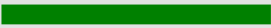

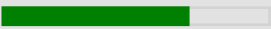

NetDiligence stores your assessment results online, so it's easy to re-evaluate your risk posture regularly and monitor changes over time. As your organization grows, new threats emerge and lawsuits multiply—you **keep your company protected**.

To learn more about how we can help your organization develop and maintain a sound cyber risk management strategy, call us at **610.525.6383** or email us at [NetDiligence Sales](#).




### 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.




Section	Summary	Scores	Issues
1 Security Policy A written policy document should be available to all employees responsible for information security.	Ok	Your score 90%	Issue
2 Security Organization To manage information security within the organization, a management framework should be established..	Ok	Your score 60%	No issue
3 Information Asset Classification and Control To maintain appropriate protection of organizational assets and, to ensure that information assets r...	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 a...	Ok	Your score 100%	No issue
5 Physical and Environmental Security To prevent unauthorized access, damage and interference to IT services. To prevent loss, damage or c...	Ok	Your score 100%	No issue
6 Communications and Operations Management To ensure the correct and secure operation of computer and network facilities. To minimize the risk ...	Ok	Your score 100%	No issue

Section	Summary	Scores	Issues
7 Access Control To control access to business information. To prevent unauthorized computer access. To prevent unaut...	Ok	Your score 80% 	Issue
8 Systems Development and Maintenance To ensure that security is built into IT systems. To ensure that IT projects and support activities ...	Ok	Your score 80% 	N/A
9 Business Continuity Management To have plans available to counteract interruptions to business activities, resulting from network a...	Ok	Your score 100% 	No issue
10 Compliance Compliance with legal requirements, to mitigate breaches of any statutory, criminal or civil obligat...	Ok	Your score 85% 	No issue
11 Privacy To ensure that there is general awareness of privacy issues surrounding data and information managem...	Ok	Your score 69.5% 	No issue
Score Average and Total Issue Sections		Your score 87.7% 	

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.