



eRisk Assessment by NetDiligence



Print this Page

eRisk Assessment - demo2 test

[Back to Dashboard](#)

Company Name: CyberBank
Invitation sent to: Mark Greisiger
Submitted: 2007-06-12 10:50:24.0

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 of questions and your responses (including text-based) in the dashboard.

Disclaimer:

This e-Risk 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 eRisk 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.

Current 'all other' customer population = 7

	Summary	Score	Issue	Comparison To Others
Security Policy	OK	100.0%		82.5%
Description:	Your Score: 100.0%			
A written policy document should be available to all employees responsible for information security.	Comparison To Others: 82.5%			
Security Organization	OK	100.0%		62.5%
Description:	Your Score: 100.0%			
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	Comparison To Others: 62.5%			
Information Asset Classification and Control	OK	60.0%	N/A	55%
Description:	Your Score: 60.0%			
To maintain appropriate protection of organizational assets and, to ensure that information assets receive an appropriate level of protection.	Comparison To Others: 55%			
Personnel Security	OK	75.0%	N/A	68.8%
Description:	Your Score: 75.0%			
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.	Comparison To Others: 68.8%			
Physical and Environmental Security	OK	100.0%		66.9%
Description:	Your Score: 100.0%			
To prevent unauthorized access, damage and interference to IT services. To prevent loss, damage or compromise of assets and interruption to business activities.	Comparison To Others: 66.9%			
Communications and Operations Management	OK	60.0%		67.5%
Description:	Your Score: 60.0%			
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.	Comparison To Others: 67.5%			
Access Control	Weak	40.0%		55%
Description:	Your Score: 40.0%			
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.	Comparison To Others: 55%			
Systems Development and Maintenance	Weak	40.0%		62.5%
Description:	Your Score: 40.0%			
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.	Comparison To Others: 62.5%			
Business Continuity Management	OK	100.0%		74.4%
Description:	Your Score: 100.0%			
To have plans available to counteract interruptions to business activities, resulting from network attacks or outages.	Comparison To Others: 74.4%			
Compliance	OK	75.0%	N/A	68.8%
Description:	Your Score: 75.0%			
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.	Comparison To Others: 68.8%			
Intellectual Property Management and Liability Avoidance	OK	100.0%	N/A	52.5%
Description:	Your Score: 100.0%			
To ensure there is a general awareness of potential legal liability resulting from website related activities that may result in the potential infringement of 3rd party intellectual property. To verify procedures and processes to mitigate the same.	Comparison To Others: 52.5%			
Privacy	OK	100.0%		62.5%
Description:	Your Score: 100.0%			
To ensure that there is general awareness of privacy issues surrounding data and information management, based on recognized Fair Information Principles including - Privacy policy Notice and Awareness; Customer Choice and Consent; Customer access; Privacy policy enforcement and accountability.	Comparison To Others: 62.5%			
Score Average and Total Issue Sections	OK	79%	3	65%
	Your Score: 79%			
	Comparison To Others: 65%			

[Back to Dashboard](#)

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.
- 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.



[Privacy Policy](#) | [Contact Us](#)

All material, Copyright NetDiligence, 2004. All rights reserved.