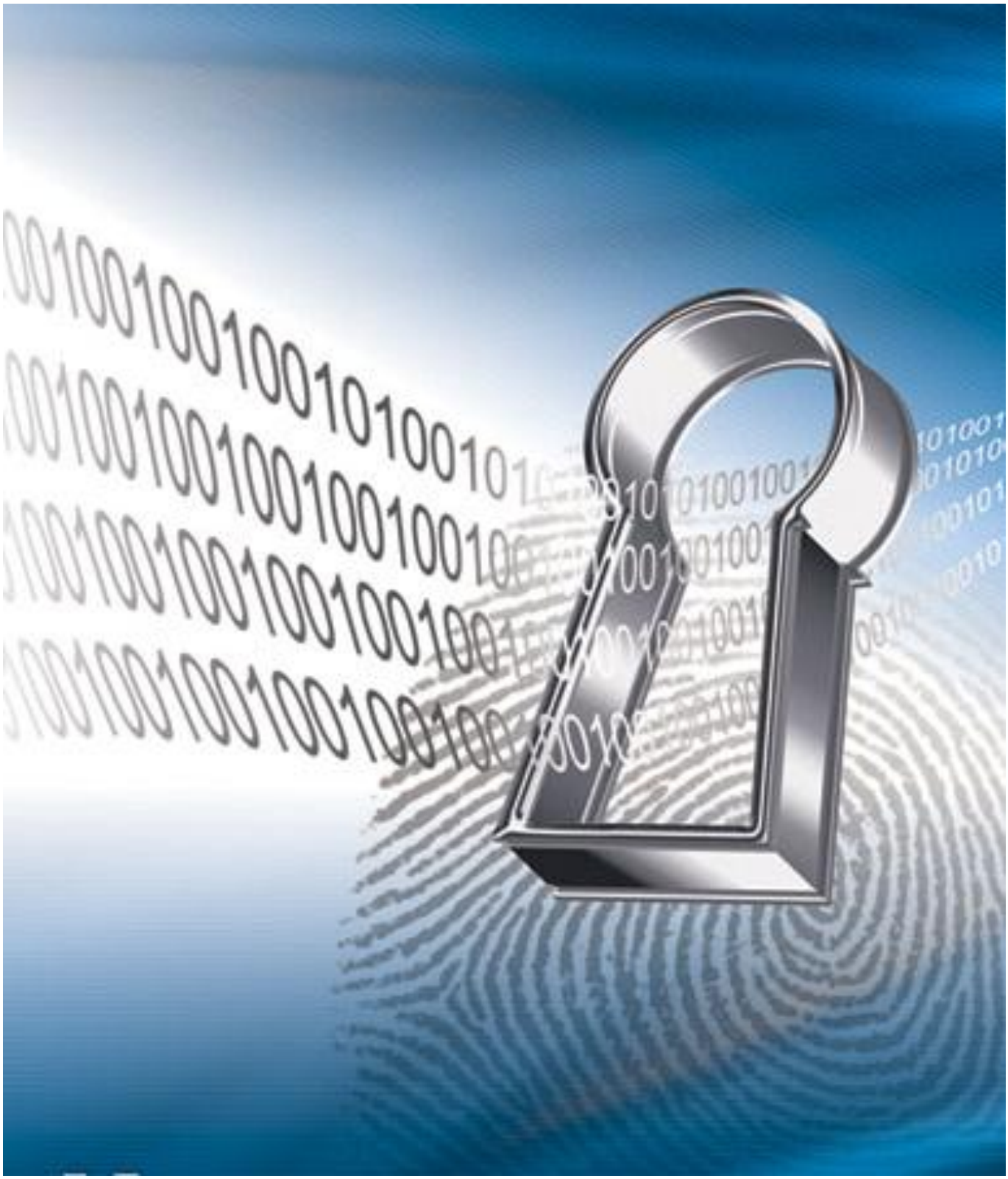

SECURITY RISK ASSESMENT REPORT FOR YOUR SELECT COMPANY

Scope of Assessment Project

NAME OF ORGANIZATION:	
LOCATION:	
ADDRESS:	
TYPE OF BUSINESS:	
IF CO-LOCATED:	
DATE OF ASSESMENT:	
REASON FOR ASSESMENT:	

Author Contact Info:

NAME:	
EMAIL ADDRESS:	

Client Contact Info:

NAME :	
EMAIL ADDRESS	

GUIDE TO THE REPORT:

The Security Status on page 3 shows how the location meets or fails the Industry Standard Practice criteria's. Whenever the location does not meet the criteria, a page reference number is given for relevant findings and the mitigation details, if applicable.

The Threat Profile on page 30 lists the threats identified for the location and protective measures to defend against these threats. Whenever a threat could be exploited, a page reference is given for the relevant finding and its mitigation details.

The Findings and Action Items Summary on page 31 lists all the findings identified at the location and gives a short summary of the actions to be taken to mitigate the corresponding threat.

The Findings section on page 34 gives detailed description of all the findings, with photographs, where applicable, their relevance to the criteria and the threat profile. Also a risk rating is assigned to individual findings based on ease of exploitation and the corresponding business impact.

Mitigation Tracker on page 58 is a table listing the actions to be taken in order to mitigate the identified findings. The action items have a

SECURITY STATUS:

NO	CRITERIA LABEL	SUMMARY OF FINDINGS	STATUS	MITIGATION DETAILS
Section 1: Security Policy – Management direction and support for information security in accordance with business requirements and relevant laws and regulations				
1.	Is the information security policy document approved by management and published and communicated to all employees and relevant external parties?	Multiple channels for desiminating this information, including RFPs, employee handbook, and Intranet updates and documents. Security items are also communicated during training of employees. IT provides this portion of training.	Meets Criteria	
2.	Is your security policy reviewed at planned intervals or when significant changes occur to ensure its continuing suitability, adequacy, and effectiveness?	Changes are updated to all channels.	Meets Criteria	
3.	Are employees required to document receipt and understanding of the security policies?	Yes. Verified during site visit.	Meets criteria	
4.	Have all employees received their own copy of the Security Policies?	Yes. Verified during site visit.	Meets Criteria	
Section 2: Organization of Information Security – The following questions concern your approach to management of information security within the organization				
5.	How management actively supports security within your organization through clear direction, demonstrated commitment and acknowledgement of information security responsibilities?			

6.	Explain how information security responsibilities are clearly defined throughout the organization?			
7.	How does the organization assure the independent review of information security and its implementation)i.e. controls, policies, processes, and procedures) at planned intervals, or when significant changes to the security implementation occur?			
8.	What policy defines the necessary security controls and agreements with third parties involving accessing, processing, communicating or managing your organization's information or information processing facilities?			
9.	Are all assets clearly identified, inventoried, assigned an owner and covered by acceptable use rules?			
10.	Describe how your organization classifies information and implements appropriate procedures for information labeling and handling?	Information is dictated by the executive team and information is protected in NTFS folders or databases using the appropriate access permissions.	Meets criteria	
Section 4: Human Resources Security – Company's your approach to ensure that employees, contractors and third party users understand their security responsibilities and are suitable for their roles.				
25.	What ensures that invalid access attempts and other security related activities are centrally reported, logged and assessed??	IT Department	Fails Criteria	On page 35
26.	What ensures that invalid access attempts and other security-related activities are investigated, including root-cause analysis and Escalated as	IT Department	Fails Criteria	On page 36

	appropriate?			
27.	What ensures that access logs are maintained in a secured and controlled manner?	IT Department	Fails Criteria	On page 37
	A. What ensures all people with access to the data center/computer equipment, including administrators and maintenance/custodial personnel, are:			
28.	Uniquely identified?	Key card has unique identifier.	Meets Criteria	
29.	Approved by management?	IT Dept and appropriate Manage	Meets Criteria	
30.	Given the least access necessary to perform their responsibilities?	IT Dept and appropriate Manage	Meets Criteria	
31.	Only current employees or partners, including the distinguishing between the two?	Key card.	Meets Criteria	
32.	Maintained (including the removal of access rights upon termination)?	IT Department	Meets Criteria	
33.	Reviewed, as being appropriate on a regular basis?	Reviews are made when an employee changes roles and annually.	Meets Criteria	
34.	What ensures that the data center is protected during non-working hours and other periods of inactivity?	Key card - combination lock.	Meets Criteria	
35.	What ensures that the Network and Computer Equipment is secure?	Key card - combo lock	Meets criteria	
36.	Does your equipment have its own rack or cabinet?	Yes.	Meets criteria	
37.	Are there locks on rack's and cabinets?	No	Fails Criteria	On page 38
38.	Is there fire suppression in the cabinet/equipment room?	No.	Fails Criteria	On page 39
39.	Fire, smoke and intrusion alarms?	Yes	Meets criteria	
40.	Are there controls for console access (screen savers or keyboard locks)?	No	Fails criteria	On page 40
41.	Are there 24 x 7 network support personnel available?	No	Fails Criteria	On page 41
42.	What ensures dependable alternate power in case the main power supply is	On site generator	Meets Criteria	

	out?			
43.	What ensures dependable alternate hardware/communications equipment/data feeds for contingency?	UPS backup power supplies and generators, if more extensive, then would need to get into complex disaster recovery scenarios.	Meets criteria	
44.	What ensures that appropriate and conditioned power 9e.g. Dual power feeds into building, stand by generators, UPS) is available for critical applications?	Backup generators, independent circuits and UPS devices.	Meets criteria	
45.	What ensures the proper shutdown of computing equipment in case of emergency?	Alerts are sent to personel. These systems can be shut-down remotely or locally.	Fails Criteria	On page 42
46	Do you conduct a regular assessment of the uninterruptible power supply (UPS) capacities to provide sufficient power for the system(s) it supports?	Yes	Meets criteria	
47	Do you have a formal UPS test program?	Yes	Meets criteria	
48	Is there a regular assessment of the power feed to the facility?	Yes	Meets criteria	
49	What ensures sufficient measures are in place to minimize damages or business interruption caused by fire and/or flood?	Business continuity plan is approved and distributed	Meets criteria	
50	What ensures that computing equipment is protected from environment related factors such as dust, heat and humidity?	Dataroom has it's own air-conditioning unit. We do not run a clean-room if that is what you are asking in regards to dust?	Meets criteria	
51	Is regular maintenance performed on all computing equipment?	No. Only when it is broke.	Fails criteria	On page 43
52	What ensures that appropriate personnel know what to do in the event of fire/flood or other emergency?	We have mandantory fire drills and systems setup in place	Meets criteria	

		internally.		
53	Are there fire, smoke and intrusion alarms?	Yes.	Meets criteria	
54	How are power, telecommunications, and network cabling protected from unauthorized access and possible damage?	Best possible	Meets criteria	
55	Are visitor logs maintained for each sensitive or critical area?	No	Fails criteria	On page 44
56	Are maintenance personnel accompanied at all times within the facility?	No	Fails criteria	On Page 45
57	Are entrances and exits monitored to prevent unauthorized removal of company or customer property?	We do not have anyone standing there no, nor do we have cameras at those places currently.	Fails criteria	On Page 46
58	How do we ensure that the location of the data center/computer equipment is not advertised?	Not advertised except for job interviews	Meets criteria	
59	Information security certifications held (FDA, HIPAA, SOX, ISO 17799 or other)?	N/A	N/A	
60	Are there required or regular IT/IS audits conducted by 3rd Party organizations at your company or site?	No	Meets criteria	
61	Other physical capabilities in place	N/A	N/A	
Section 6: Communication and Operations Management – Controls to ensure the correct and secure operation of information processing facilities.				
62	Methods to assure that operating procedures are documented , maintained and are available to all users who need them	Employee Handbook and IT Training, Any changes are made are communicated via email.	Meets criteria	
100	Describe the formal policies, procedures, agreements and controls in place to protect information media against unauthorized access, misuse or corruption during transportation beyond your organizations physical boundaries	Transportation off-site of sensitive data on occurs through the FTP mechanism.	Meets criteria	

101	Describe the formal policies, procedures, agreements and controls in place to protect information associated with the interconnection of business information systems	N/A	N/A	
	A. Define your organization's procedures to ensure the security of electronic Information passing over public networks from fraudulent activity, contract dispute and unauthorized disclosure and modifications			
102	Describe the formal policies, procedures, agreements and controls in place to protect information involved in on-line transactions to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or relay	All sensitive data is protected via 128-bit SSL encryption. Websense provides additional protection against message alteration.	Meets criteria	
103	Does your website have a privacy/legal notice?	Yes	Meets criteria	
104	Have security/audit personnel reviewed the security configuration of the web server?	No	Fails criteria	On page 47
105	Does your website have a privacy/legal notice?	Yes	Meets criteria	
106	Where is the web server located (DMZ, Internal)	DMZ	Meets criteria	
107	Do you operate the web server in a separate partition from the operating system files?	Yes	Meets criteria	
108	Do you scan your web servers periodically with vulnerability detection tools?	No	Fails criteria	On page 48
109	How do you address web server vulnerabilities?	IIS has built-in lock down tools, additionally auto Windows Updates for Critical patches, best practices documentation and Websense Security Suite.	Fails criteria	On page 49
110	Have installation default document trees been removed from all servers?	Yes	Meets criteria	
111	Is the web server remotely administered?	No	Meets criteria	

112	Are your Web server operating system access controls used to assure that Web content files being read are not written by Web service processes?	Yes	Meets criteria	
	G. Define your organization's procedures to ensure the detection of unauthorized information processing activities			
113	Describe the formal policies, procedures, and controls in place to assure audit logs are used to record user activities, exceptions, and information security events	Using Windows auditing, alerts that meet certain conditions are sent to IT dept.	Meets criteria	
114	Describe the formal policies, procedures, and controls in place for monitoring the use of information processing facilities and that the activities are revived regularly	Need additional info	N/A	
115	Describe the formal policies, procedures, and controls in place to assure faults are logged, analyzed, appropriate actions is taken and the logs are not tampered with	Logged to a special monitoring system that is only accessed by IT dept.	Meets criteria	
116	Describe the formal policies, procedures, and controls in place to assure the clocks of all relevant information processing systems within your organization or security domain are synchronized with an agreed accurate time source	Alerts are sent if any of the systems lose a connection to the Network Time Server. All PCs and Servers have a Network Time Server and all the Cisco devices have a Network Time Server. All systems are in sync.	Meets criteria	

117	What information are you currently logging on your systems (i.e. logon/logoff, critical file access, account creation, user rights, user and group management, security policy changes, unauthorized access attempts, restart/shutdown)	Logon/logoff, our system uses an access front end to pull data from SQL server. Data is not stored elsewhere at this time.	Meets criteria	
118	What is your log retention policy?	Each have various thresholds based on size limitations.	Meets criteria	
119	What audit reports are produced?	Logon/logoff, read/write/modify files.	Meets criteria	
Section 7: Access Control – The following questions concern your controls to ensure authorized user access and prevent unauthorized access to information systems.				
	A. Describe how your access control policies and procedures assure access are established based on business and security requirements			
120	Is there a formal user registration and re-registration procedure in place for granting, revoking and regularly reviewing access to all information systems and services?	Yes	Meets criteria	
121	Describe the process for assuring the allocation and use of privileges are restricted and controlled	Each department has a list of resources required to perform their job functions. The network is divided into various sections for these requirements, the user is then given the permission that will only allow them access to those areas.	Meets criteria	
	B. Describe your password policy			

122	What is the minimum password length required?	8 characters	Meets criteria	
123	What is the password complexity? (i.e. upper/lower case, letters, numbers, and special characters)	Microsoft's Password Complexity Requirements	Meets criteria	
124	Do you force the initial or reset password to be changed?	Yes.	Meets criteria	
125	What is your password expiration requirement? (i.e. 30, 60, 90 days)	45 days	Meets criteria	
126	How do you deliver distribute initial or reset passwords?	We give new users a temporary password which they then change during first logon.	Meets criteria	
127	Does your security policy allow sharing of accounts and passwords?	No	Meets criteria	
128	Are password encrypted in storage or transit?	Yes	Meets criteria	
129	What is the password reset process for accountability and monitoring?	Temporary password is given to user to reset, then the user changes password next logon.	Meets criteria	
130	Are passwords embedded in logon scripts?	No	Meets criteria	
131	Do you change all default passwords?	Yes	Meets criteria	
	C. Describe the formal policies, procedures, and controls in place to prevent unauthorized access to operating systems			
132	Has the security configuration of the operating system been reviewed by security audit personnel?	Yes	Meets criteria	
133	Have all servers that receive, transmit and store data been consistently configured?	Yes	Meets criteria	
134	Has the following been documented: O/S version, O/S patches and dates of patch, listing of software titles on system?	Yes	Meets criteria	
135	Please define what privileged accounts are set up on each class of system	Domain Administrators	Meets criteria	
136	How many personnel have elevated privileges ?	IT and Development	Meets criteria	

167	How much application detail information your error message reveals?	None	Meets criteria	
168	Do you return friendly error information to end-users?	Yes	Meets criteria	
169	Do you pass valuable exception information back to the caller?	Nothing	Meets criteria	
170	Do your applications fail gracefully?	Yes	Meets criteria	
	D. Describe the formal policies, procedures, and controls in place to prevent unauthorized access to information held in a database system			
171	What database technology is being used?	Microsoft SQL Server	Meets criteria	
172	Which applications access the database?	Access	Meets criteria	
173	How is access to the data limited/controlled (database administrators, specific applications and limited system administrators) ?	By use of usernames and passwords	Meets criteria	
174	Is confidential data stored encrypted and/or encrypted in transit?	Only encrypted if VPN off-site.	Fails criteria	On page 51
175	Is data sourced from other databases?	No	Meets criteria	
177	Is the mechanism secure?	N/A	Meets criteria	
178	How applications connect to databases? (ODBC, TGADP, SQLNet, RDO)	ODBC	Meets criteria	
179	Are all usernames and passwords that connect to databases stored encrypted and in a protected area?	Yes	Meets criteria	
180	Are there any special IDs (such as the installation ID) used with the database?	No	Meets criteria	
181	What permissions has been granted to these ID's?	N/A	Meets criteria	
182	What is your database fail over procedure?	Clustering locally and replication remotely.	Meets criteria	
183	Is the database file system shared anywhere?	No	Meets criteria	
184	How are connections to the database protected?	LAN	Meets criteria	
185	How many DBA's have access to the database?	Two	Meets criteria	
186	Who has access to backup privilege?	Two backup	Meets criteria	

		accounts		
187	Is backup automated?	Yes	Meets criteria	
188	Does your database have his own server/schema/instance?	Yes	Meets criteria	
189	Can users, other than the DBA, make changes to the database without using application-stored procedures?	No	Meets criteria	
190	How do you secure your database error logs?	Password protected	Meets criteria	
	E. Describe the formal policies, procedures and appropriate security measures in place to protect against the risk of using mobile computing, tele-working and communication facilities?			
191	Whether there exists a procedure for handling the storage of information: Does this procedure address issues such as information protection from unauthorised disclosure or misuse?	Yes	Meets criteria	
192	Whether the system documentation is protected from unauthorised access.	Yes	Meets criteria	
193	Whether the access list for the system documentation is kept to minimum and authorised by the application owner. Example: System documentation need to be kept on a shared drive for specific purposes, the document need to have Access Control Lists enabled (to be accessible only by limited users.)	Yes	Meets criteria	
194	Whether there exists any formal or informal agreement between the organisations for exchange of information and software.	As needed	Meets criteria	
195	Whether the agreement does addresses the security issues based on the sensitivity of the business information involved.	Yes	Meets criteria	
196	Whether security of media while being transported taken into account.	Yes	Meets criteria	
197	Whether the media is well protected from unauthorised access, misuse or corruption.	Yes	Meets criteria	

198	Whether Electronic commerce is well protected and controls implemented to protect against fraudulent activity, contract dispute and disclosure or modification of information.	Yes	Meets criteria	
199	Whether Security controls such as Authentication, Authorisation are considered in the ECommerce environment.	Yes	Meets criteria	
200	Whether electronic commerce arrangements between trading partners include a documented agreement, which commits both parties to the agreed terms of trading, including details of security issues.	Yes	Meets criteria	
201	Whether there is a policy in place for the acceptable use of electronic mail or does security policy does address the issues with regards to use of electronic mail.	No	Fails criteria	On page 52
202	Whether controls such as antivirus checking, isolating potentially unsafe attachments, spam control, anti relaying etc., are put in place to reduce the risks created by electronic email.	Yes	Meets criteria	
203	Whether there is an Acceptable use policy to address the use of Electronic office systems.	No	Fails criteria	On page 53
204	Whether there are any guidelines in place to effectively control the business and security risks associated with the electronic office systems.	Following industry standard practice	Meets criteria	
205	Whether there is any formal authorisation process in place for the information to be made publicly available. Such as approval from Change Control which includes Business, Application owner etc.,	Yes	Meets criteria	

	A. Describe how timely information about technical vulnerabilities of information systems being used is obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk			
225	Do you have a formal patch process for all systems?	All systems are patched automatically except for sensitive systems that need to be tested, these patches are run on test machines and checked for stability.	Meets criteria	
226	Are software updates distributed electronically from a central facility?	Yes	Meets criteria	
227	Are security patches applied in a timely manner?	Yes	Meets criteria	
228	Discuss testing of new patches (functional and interoperability testing)	A test server that best replicates a production server is used to test patches.	Meets criteria	
229	Are third party security or internal audits performed?	No. Only internal.	Fails criteria	On page 54
230	When was the last audit performed?	Audits internally are performed based on the availability of staff.	Meets criteria	
231	Please provide a copy of the last audit results. Have findings been corrected?	Yes	Meets criteria	
232	Did the audit cover all the systems, including the ISP?	We do not audit our ISP.	N/A	
233	Has a penetration test been performed?	No. Only timelines of patches and Anti-Virus	Fails criteria	On page 55
234	Who performed the penetration testing?	N/A	N/A	
235	May we review the results?	Yes	In conclusive	
236	Discuss your processes and solutions against exploits.	We wait for security patches to be released. No protection against zero day exploits	Fails criteria	On page 56

THREAT PROFILE :

THREAT ID:	DESCRIPTION:	STATUS:	MITIGATION DETAILS:
T1.	Major hardware – server or workstation – stolen	Safe	
T2.	Minor hardware – backup tape, USB memory stick – stolen or destroyed	Unsafe	See page __
T3.	Power blackout	Safe	
T4.	Communications or equipment failure	Safe	
T5.	Zero day Web Server, SQL, or OS exploit	Unsafe	See page 58
T6.	Brute Force / Reverse Brute Force Attack	Safe	
T7.	Email Phishing of company email system	Unsafe	See page __
T8.	Flood	Unsafe	See page __
T9.	Fire	Safe	
T10.	Civil unrest	Safe	
T11.	Terrorist attack	Unsafe	See page __

FINDINGS AND ACTION ITEMS SUMMARY:

The following security vulnerabilities where found:

VULNERABILITY ID:	DESCRIPTION:	RISK RATING:	MITIGATION DETAILS:
1.	Access to equipment room is unrestricted and not controlled separately from the rest of the facility	Medium Risk	See page 34
2.	No proper recording and logging of failed access attempts. Logs are stored on a database server, easily accessible. A perpetrator can easily sanitize or delete them.	High Risk	See page 35
3.	No regular checks of logs. Failed or successful attempts may go unnoticed	High Risk	See page 36
4.	Logs are not secured properly?	High Risk	See page 37
5.	No locks on racks and cabinets?	Medium Risk	See page 38
6.	No separate fire suppression system in cabinets or computer room?	Medium Risk	See page 39
7.	No screen savers and keyboard locks are used	High Risk	See page 40
8.	No network support personnel available at all times?	High Risk	See page 41
9.	No proper equipment shut down in case of emergency?	Medium Risk	See page 42

10.	Regular maintenance is not performed on computers. They are serviced only in case of break down	Medium Risk	See page 43
11.	No separate visitor logs for computer equipment room.	Medium Risk	See page 44
12.	Maintenance personnel is not accompanied at all times within the facility	High Risk	See page 45
13.	Entrances/exits are not monitored at all times for unauthorized removal of company property	High Risk	See page 46
14.	No review of security configuration of the Web Server by a security specialist, as a second opinion	High Risk	See page 47
15.	No periodic scans for vulnerabilities of the Web Server	High Risk	See page 48
16.	Mitigation of vulnerabilities	High Risk	See page 49
17.	No connection time restrictions	Medium Risk	See page 50
18.	Confidential data is stored unencrypted	High Risk	See page 51
19.	No Acceptable use policy for email	Medium Risk	See page 52
20.	No acceptable use policy for use of electronic office systems	High Risk	See page 53
21.	No third party security audits. Only internal	Medium Risk	See page 54

22.	No penetration testing was ever performed	High Risk	See page 55
23.	No procedure in place for remediation of vulnerabilities with known exploits till release of security patch	High Risk	See page 56
24.	No plan for IDS configuration and rules updates	High Risk	See page 57

FINDINGS :

1. No access restriction separates the computer room from the rest of the facility

RISK
MEDIUM

RELEVANT TO WHICH SECURITY CRITERIA:	20. - No access restriction separates the computer room from the rest of the facility
RELEVANT TO WHICH THREATS IN THE SECURITY PROFILE:	T1. Major hardware – server or workstation - stolen.
IMPACT:	High
EASE OF EXPLOITATION:	Medium

Exploit: Perpetrator pick's up equipment and walks out.

2 . What ensures that invalid access attempts and other security related activities are centrally reported, logged and assessed?

Repeated unsuccessful system compromise attempts and break-ins may go unnoticed for long times.

RISK
HIGH

RELEVANT TO WHICH SECURITY CRITERIA:	25. What ensures that invalid access attempts and other security related activities are centrally reported, logged and assessed?
RELEVANT TO WHICH THREATS IN THE SECURITY PROFILE:	T5. Zero day Web Server, SQL, or OS exploit T6. Reverse Brute Force Attack
IMPACT:	High
EASE OF EXPLOITATION:	Very Easy

Exploit: Log in attempt numbers are limited per account. If an attacker try's the same password, say the company name, the street name of the main company office location or the name of a successful company product, as password to all user names from the company phone directory, he will not be restricted by the number of failed login attempts, since he is attempting to log in to all user names.

3. What ensures that invalid access attempts and other security-related activities are investigated, including root-cause analysis and Escalated as appropriate?

RISK LEVEL
HIGH

RELEVANT TO WHICH SECURITY CRITERIA:	26. What ensures that invalid access attempts and other security-related activities are investigated, including root-cause analysis and Escalated as appropriate
RELEVANT TO WHICH THREATS IN THE SECURITY PROFILE:	T5. Zero day Web Server, SQL, or OS exploit T6. Reverse Brute Force Attack
IMPACT:	HIGH
EASE OF EXPLOITATION:	Very Easy

Exploit: Log in attempt numbers are limited per account. If an attacker try's the same password, say the company name, the street name of the main company office location or the name of a successful company product, as password to all user names from the company phone directory. He will not be restricted by the number of failed login attempts, since he is attempting to log in to all user names. If logs are not reviewed daily or every two days, the attacker has a large window of opportunity to try new attempts. It is common that Reverse brute force is started just before midnight and continued after. As a result the number of failed attempts can be doubled. Also is the potential consequence that the persistent attacker will exhaust the number of unsuccessful attempts and will lock all computers at your company.

4. What ensures that access logs are maintained in a secured and controlled manner?

.

RISK LEVEL
HIGH

RELEVANT TO WHICH SECURITY CRITERIA:	27. What ensures that access logs are maintained in a secured and controlled manner?
RELEVANT TO WHICH THREATS IN THE SECURITY PROFILE:	T5. Zero day Web Server, SQL, or OS exploit T6. Reverse Brute Force Attack
IMPACT:	High
EASE OF EXPLOITATION:	Easy

Exploit: After successful attack, the perpetrator will be able to clean the logs and remove traces documenting his criminal activity.

5. Are there lock's on racks and cabinets?

.

RISK LEVEL
MEDIUM

RELEVANT TO WHICH SECURITY CRITERIA:	37. Are there lock's on racks and cabinets?
RELEVANT TO WHICH THREATS IN THE SECURITY PROFILE:	T2. Major hardware – server or workstation - stolen
IMPACT:	High
EASE OF EXPLOITATION:	Easy

Exploit: A visitor walks away with a blade server in his Portfolio Holder or one temporary replacement cleaning staff hides the server between garbage bags.

6. Is there separate, dedicated fire suppression in the computer room?

A defective toaster may trigger the sprinkler system, ending in spraying water on all racks with computer equipment.

RISK LEVEL
MEDIUM

RELEVANT TO WHICH SECURITY CRITERIA:	37. Is there separate, dedicated fire suppression in the computer room?
RELEVANT TO WHICH THREATS IN THE SECURITY PROFILE:	T2. Power blackout T3. Communications failure
IMPACT:	High
EASE OF EXPLOITATION:	No

Exploit: None.

7. There are no controls for console access (screen savers or keyboard locks).

Since visitor logs are not maintained for each sensitive or critical area and maintenance personnel is not accompanied at all times within the facility, this can be abused.

There is no firewall or VPN that can prevent this. With an inexpensive USB memory stick and free access to the KVM, a visitor can simply copy valuable customer or product development data and walk out right through the front door.

The very private and confidential information that companies depend on to create competitive advantage, and the information government regulations require be kept secure, can fit easily inside a pocket.

RISK LEVEL
HIGH

RELEVANT TO WHICH SECURITY CRITERIA:	40. - Are there controls for console access (screen savers or keyboard locks)?
RELEVANT TO WHICH THREATS IN THE SECURITY PROFILE:	
IMPACT:	HIGH
EASE OF EXPLOITATION:	Yes

Exploit: Cleaning staff or maintenance personnel can create an account for remote access and abuse..

8. No technical support available 24/7

RISK
HIGH

RELEVANT TO WHICH SECURITY CRITERIA:	45. - No technical support staff is on site 24/7 for emergency shut down. Alerts are sent to personel. These systems can be shut-down remotely or locally. However nothing ensures the proper shutdown of computing equipment in case of emergency?
RELEVANT TO WHICH THREATS IN THE SECURITY PROFILE:	T3. - Power blackout
IMPACT:	High
EASE OF EXPLOITATION:	Medium

Exploit: Minor storm can take the business off line..

9. **- No regular maintenance is performed on the computer equipment.**

RISK
MEDIUM

RELEVANT TO WHICH SECURITY CRITERIA:	51 – No regular maintenance is performed on the computing equipment. Maintenance is performed only when it is broke.
RELEVANT TO WHICH THREATS IN THE SECURITY PROFILE:	T1. Major hardware – server or workstation - stolen.
IMPACT:	High
EASE OF EXPLOITATION:	Medium

Exploit: Perpetrator pick's up equipment and walks out.

10. - No visitor logs are maintained for each sensitive or critical area.

RISK
MEDIUM

RELEVANT TO WHICH SECURITY CRITERIA:	55 – No visitor logs are maintained for each sensitive or critical area.
RELEVANT TO WHICH THREATS IN THE SECURITY PROFILE:	T1. Major hardware – server or workstation - stolen. T2 – Minor hardware – hard drive, memory stick or back-up tape – stolen.
IMPACT:	High
EASE OF EXPLOITATION:	Medium

Exploit: Perpetrator pick's up equipment and walks out.

11. - No visitor logs are maintained for each sensitive or critical area.

RISK
MEDIUM

RELEVANT TO WHICH SECURITY CRITERIA:	55 – No visitor logs are maintained for each sensitive or critical area.
RELEVANT TO WHICH THREATS IN THE SECURITY PROFILE:	T1. Major hardware – server or workstation - stolen. T2 – Minor hardware – hard drive, memory stick or back-up tape – stolen.
IMPACT:	High
EASE OF EXPLOITATION:	Medium

Exploit: Cleaning staff unplugs something and as a result the on line business goes off line..

12 - Maintenance personnel are not accompanied at all times within the facility

RISK
HIGH

RELEVANT TO WHICH SECURITY CRITERIA:	56 - Maintenance personnel are not accompanied at all times within the facility.
RELEVANT TO WHICH THREATS IN THE SECURITY PROFILE:	T1. Major hardware – server or workstation - stolen.
IMPACT:	High
EASE OF EXPLOITATION:	Medium

Exploit: Perpetrator pick's up equipment and walks out.

13. Access to the facility

RISK
HIGH

RELEVANT TO WHICH SECURITY CRITERIA:	57 - Entrances and exits are not monitored to prevent unauthorized removal of company or customer property. Nobody is standingat entrances and there are no cameras at those places currently.
RELEVANT TO WHICH THREATS IN THE SECURITY PROFILE:	T1. Major hardware – server or workstation - stolen.
IMPACT:	High
EASE OF EXPLOITATION:	Medium

Exploit: Perpetrator pick's up equipment and walks out.

14. – **No security audits has been performed by security personnel**

RISK
HIGH

RELEVANT TO WHICH SECURITY CRITERIA:	104 – No security/audit personnel reviewed the security configuration of the web server
RELEVANT TO WHICH THREATS IN THE SECURITY PROFILE:	T5. - Zero day Web Server, SQL, or OS exploit
IMPACT:	High
EASE OF EXPLOITATION:	Medium

Exploit: Sooner or later, hackers will do the “audit” which they call successful penetration.

15. - **No periodic scans of the Web server with vulnerability detection tools.**

RISK
HIGH

RELEVANT TO WHICH SECURITY CRITERIA:	108 - Do you scan your web servers periodically with vulnerability detection tools?
RELEVANT TO WHICH THREATS IN THE SECURITY PROFILE:	T5. - Zero day Web Server, SQL, or OS exploit
IMPACT:	High
EASE OF EXPLOITATION:	Medium

Exploit: Hackers may like your server, a lot.

16. **No monitoring of server security and logging.**

RISK
HIGH

RELEVANT TO WHICH SECURITY CRITERIA:	109 - To address web server vulnerabilities only IIS built-in lock down tools, Windows Updates for Critical patches, best practices documentation and Websense Security Suite are only used at this time.
RELEVANT TO WHICH THREATS IN THE SECURITY PROFILE:	T5. - Zero day Web Server, SQL, or OS exploit.
IMPACT:	High
EASE OF EXPLOITATION:	Medium

Exploit: A hacker can test Zero Day exploits..

17. There are no restrictions on connection times

RISK
MEDIUM

RELEVANT TO WHICH SECURITY CRITERIA:	140 - There are no established restrictions on connection times to provide additional security for high risk applications. Users are allowed to work after-hours. There are no restriction on connection times, on idle times.
RELEVANT TO WHICH THREATS IN THE SECURITY PROFILE:	T5. - Zero day Web Server, SQL, or OS exploit
IMPACT:	High
EASE OF EXPLOITATION:	Medium

Exploit: A hacker can roam through the network during off hours. He will still need a vulnerability to exploit. That makes this vulnerability of Medium Risk.

18. **– Confidential data is not stored encrypted**

RISK
HIGH

RELEVANT TO WHICH SECURITY CRITERIA:	174 - Confidential data IS NOT stored encrypted and/or encrypted in transit. Only encrypted if VPN off-site
RELEVANT TO WHICH THREATS IN THE SECURITY PROFILE:	T1. Major hardware – server or workstation - stolen.
IMPACT:	High
EASE OF EXPLOITATION:	Medium

Exploit: Visitor or third party maintenance staff can walk out with one of the servers or workstations..

19. - **No email use policy**

RISK
MEDIUM

RELEVANT TO WHICH SECURITY CRITERIA :	201. No email use policy
RELEVANT TO WHICH THREATS IN THE SECURITY PROFILE:	T7. - Email Phishing of company email system
IMPACT:	High
EASE OF EXPLOITATION:	Medium

Exploit: Perpetrator pick's up equipment and walks out.

20. No acceptable use policy to address the use of Electronic office systems.

RISK
HIGH

RELEVANT TO WHICH SECURITY CRITERIA:	203 – No acceptable use policy to address the use of Electronic office systems.
RELEVANT TO WHICH THREATS IN THE SECURITY PROFILE:	T6. - Brute Force / Reverse Brute Force Attack
IMPACT:	High
EASE OF EXPLOITATION:	Medium

Exploit: A disgruntled employee may attempt a Brute Force / Reverse Brute Force Attack.

21. **No third party security audits are performed. Only internal, as time permits.**

RISK
MEDIUM

RELEVANT TO WHICH SECURITY CRITERIA:	229. - No third party security or internal audits are performed. Only internal, as time permits.
RELEVANT TO WHICH THREATS IN THE SECURITY PROFILE:	T5 - Zero day Web Server, SQL, or OS exploit.
IMPACT:	High
EASE OF EXPLOITATION:	Medium

Exploit: Perpetrator pick's up equipment and walks out.

22. No penetration test has been performed

RISK
HIGH

RELEVANT TO WHICH SECURITY CRITERIA:	233. No penetration test has been performed
RELEVANT TO WHICH THREATS IN THE SECURITY PROFILE:	T5 - Zero day Web Server, SQL, or OS exploit
IMPACT:	High
EASE OF EXPLOITATION:	Medium

Exploit: A hacker may use a new or residual vulnerability to compromise the system

23 - No procedure in place for remediation of vulnerabilities with known exploits till release of security patch

RISK
HIGH

RELEVANT TO WHICH SECURITY CRITERIA:	236. No procedure in place for remediation of vulnerabilities with known exploits till release of security patch
RELEVANT TO WHICH THREATS IN THE SECURITY PROFILE:	. T5 - Zero day Web Server, SQL, or OS exploit
IMPACT:	High
EASE OF EXPLOITATION:	Medium

Exploit: A hacker my use a Zero day Web Server, SQL, or OS exploit.

24 - No plan for IDS configuration and rules updates

RISK
HIGH

RELEVANT TO WHICH SECURITY CRITERIA:	241 - Process for updating IDS configuration and rules: There is currently no process, the IDS is configured to meet the requirements of the specific server, it runs at kernel mode and prevents unauthorized changes. It is only modified if the system changes
RELEVANT TO WHICH THREATS IN THE SECURITY PROFILE :	T5 - Zero day Web Server, SQL, or OS exploit
IMPACT:	High
EASE OF EXPLOITATION :	Medium

Exploit: A hacker my use a Zero day Web Server, SQL, or OS exploit.

MITIGATION TRACKER:

VULN. ID:	DESCRIPTION:	RISK RATING:	RESPONSIBILITY FOR FIXING:	DEADLINE FOR FIXING:	RESPONSIBILITY TO VERIFY THE RESOLUTION OF THE PROBLEM:	DEADLINE FOR VERIFYING:	CURRENT STATUS:
1.							
2.							
3.							
4.							
5.							
6.							
7.							
8.							
9.							
10.							