ORGANIZATION	Response	"Yes" Details	Severity	Risk Score	
SECURITY POLICY	**YES. NO. N/A.**	**Planned / just started. Partially completed. Fully implemented.**	**High. Medium. Low.**	**Calculated**	**Risk Upperlimit**
Have the Information Security Policies been issued to all employees, including third party personnel and contractors?	Yes	Planned / just started	Very High	2	4
Have all employees formally acknowledged adherence to the Information Security Policies?	Yes	Partially completed	Very High	1	4
Are employees required to annually re-acknowledge compliance with the Information Security Policies?	Yes	Fully implemented	Very High	0	4
How and when do you perform internal audits to measure compliance with the Information Security Policies?	Yes	Planned / just started	High	1.5	3
How frequently do you perform periodic reviews to update security policies and guidelines for relevancy and emerging topics?	Yes	Partially completed	High	0.75	3
Are controls in place to restrict your ability to transmit customer data to unauthorized personnel outside your company ?	Yes	Fully implemented	High	0	3
Has an organizational policy on copyright compliance been implemented and communicated to all users?	Yes	Planned / just started	Medium	1	2
Do you have a policy that prohibit generic logon account and do you follow the policy?	Yes	Partially completed	Medium	0.5	2
Are all the following subject to data confidentiality agreements? * Permanent employees * Contractors / temporary staff * 3rd Party service providers	Yes	Fully implemented	Medium	0	2
Has your business issued an E-mail Usage Policy ?	Yes	Planned / just started	Low	0.5	1
Do you take action against users who use e-mail in contradiction to the E-mail Usage Policy ?	Yes	Partially completed	Low	0.25	1
Has your business issued an Internet Policy? (e.g. only access the Internet for legitimate work-related purposes, no downloading of games, etc.)	Yes	Fully implemented	Low	0	1
Are all users required to sign an internet usage and responsibility agreement that acknowledges compliance with the stated Internet Policy?	No		Very High	4	4
Are there comprehensive documentation standards for IT development and operational controls?	No		High	3	3
Is there a clear desk policy ?	No		Medium	2	2
SECURITY OFFICER & ORGANIZATION					0
Do you have a full-time Information Security Officer ?	No		Low	1	1
Have roles and responsibilities for protecting assets and implementing security measures been explicitly defined and communicated to all the department/groups?	N/A		Very High		0
Has a formal risk analysis process been implemented to assist management in identifying security threats?	Yes	Fully implemented	Low	0	1

EMPLOYEE SECURITY FOCUS	Response	"Yes" Details	Severity	Risk Score	0
AWARENESS & TRAINING	YES. NO. N/A.	Planned / just started. Partially completed. Fully implemented.	High. Medium. Low.	Calculated	0
Has a formal, on-going Security Training program been implemented?					0
Have you implemented a process to measure the Effectiveness of Security Training ?					0
Does the on-going Security Awareness program include instructing users on how to detect and avoid 'social engineering' attacks as well as competitive intelligence probes?					0
Have users been educated on how to report suspected security violations or vulnerabilities?					0
Do regular bulletins sent to employees alerting them to risks and vulnerabilities involved in computing, including basic tasks such as backup, anti-virus scanning and choosing strong passwords?					0
Is there a process to communicate security policy and guideline changes to employees?					0
Is the importance of Information Security visible throughout the organization (e.g. security discussions in company meetings, security award, posters etc.)					0
Do you notify employees that customer sensitive data cannot be loaded on personal PC's?					0
Are users of systems containing sensitive information made aware of legal and company obligations associated with the use of the application? (e.g. through Logon Banner)					0
Have employees been instructed to challenge strangers or unescorted visitors in non-public areas?					0
Are there periodic spot-checks of users' workspaces to monitor compliance with the information protection program.					0
RECRUITMENT PROCESS / NEW EMPLOYEE IT ORIENTATION					0
Are new hire workers (including contractors & third party personnel) subjected to a history and background check? (e.g. References, police records, etc.)					0
Do workers receive introductory awareness security training ?					0
EMPLOYEE EXIT / TRANSFER					0
Does Human Resources (HR) department provide system administrators with a list of: * workers transferring departments * workers leaving the company					0
Is there a process to notify system administrators when workers leave the business?					0
Are exit interviews conducted to recover property given to workers? For Example: a) Cimpany property (badges, company credit cards etc). b) Tools of the job (laptops, mobile phones, pagers, remote dial-in access cards, modems etc.).					0
Is there an emergency program for immediate removal of employee's system access when the departing employee is identified as disgruntled or high risk?					0
Are access / exit controls employed in your facility?					0
When employees leave, do you 1) check to see if they have sponsored accounts or badges for guests and 2) question them on continued need AND 3) assign new sponsors?					0

CHANGE MANAGEMENT	Response	"Yes" Details	Severity	Risk Score	0
CHANGE MANAGEMENT	YES. NO. N/A.	Planned / just started. Partially completed. Fully implemented.	High. Medium. Low.	Calculated	0
Do you have documented change control procedures to manage all modifications to the development environment (software, hardware, network)?					0
Is change control preformed on an regular basis?					0
Is Physical Security (e.g. power control, locks, badges, entrance cards) part of your change control process?					0
Are Changes approved in change control documented and stored in a publicly accessible format?					0
Does the customer sign off on changes effecting them?					0
Is there a documented procedure for performing emergency changes outside the change control process?					0
NETWORK SECURITY	Response	"Yes" Details	Severity	Risk Score	0
ROUTER / FIREWALL	YES. NO. N/A.	Planned / just started. Partially completed. Fully implemented.	High. Medium. Low.	Calculated	0
Do you maintain a current network diagram and who owns and maintains it?					0
Has, at minimum, stateful firewalls been deployed at all external connections (e.g., Internet)? Give type of firewall currently used. If no, list the type of security mechanism used (e.g., router with ACL's)					0
Is the firewall(s) configured with a policy that all services are denied unless expressly permitted?					0
Do you have a process/criteria to evaluate the risk of protocols/ports before implementing them on the firewalls?					0
Is outgoing traffic directed to external proxy servers? If so, are these proxy servers resident on a DMZ?					0
Are all services forbidden except when specifically requested?					0
Is logging enabled on all firewalls, routers, and proxy servers? Is a process in place to review the logs regularly?					0
Is the firewall(s) and/or the proxy server(s) configured on a hardened platform, with limited functionality (e.g., all unnecessary applications removed)?					0
Is access to all firewalls, routers, and proxy servers restricted to only those people who need to manage these devices?					0
Do administrators remotely access the routers and/or firewalls? If So are they securely authenticated by using one-time passwords or encrypted login sessions?					0
Is there a process in place to ensure that all the routers/firewalls have the latest software and that they are patched regularly with the latest security updates from their respective vendors.					0
VPN - REMOTE USER CONNECTIVITY					0

For computers used for VPN remote access, have you implemented a Personal Firewall?					0
Do you only allow VPN access to computers that implement Anitivirus Software and Personal Firewall ?					0
Do you have a process in place in order to cancel anyone's VPN access rights as soon as their project is completed or their reason for having the VPN is invalidated?					0
APPLICATION SECURITY	**Response**	**"Yes" Details**	**Severity**	**Risk Score**	0
SECURITY IN APPLICATION DEVELOPMENT	**YES. NO. N/A.**	**Planned / just started. Partially completed. Fully implemented.**	**High. Medium. Low.**	**Calculated**	0
Does your system development methodology address information security during the discovery and development phase?					0
Do you perform a security code review during each phase of development?					0
Are there separate environments for each customer for development and testing of systems ?					0
Are all the software developers working on the software given orientation in security requirements of the customer before they start work on the project.					0
Are all developed software tested for virus by running anti-virus on them before delivering them to the customer ?					0
DATA SECURITY					0
Are backups of business critical data done regularly (at least weekly)?					0
Do you have an on-line mechanism to verify that all backups complete successfully?					0
Do you periodically restore information from backup tapes to ensure data integrity?					0
Are backup tapes kept in an environmentally controlled and secured area?					0
Do you store tapes off-site ?If yes, how is access to the tapes protected at the site?					0
Are back up tapes stored in location with physical access control?					0
Is there a regular audit conducted to account for all the backup tapes.					0
Are backup tapes ever destroyed if yes then what procedure is used to destroy them.					0
DATA CLASSIFICATION					0
Does all critical business data have an owner?					0
Is critical information classified according to a classification guideline (e.g. secure, confidential, public etc.)					0
Does access to sensitive customer data have to be authorized by the owners of the data?					0
SYSTEM SECURITY	**Response**	**"Yes" Details**	**Severity**	**Risk Score**	0
SERVER VULNERABILITY & HARDENING	**YES. NO. N/A.**	**Planned / just started. Partially completed. Fully implemented.**	**High. Medium. Low.**	**Calculated**	0
Is there a process to proactively obtain the latest security patches and updates?					0
Do you have a process to identify network, application and OS based systems vulnerabilities?					0
Do you used automated tools to assess system vulnerabilities?					0

Does your internal audit simulate outside attacks or do you hire external consultants to simulate attacks on your system to uncover its susceptibility.					0
Have all business critical systems used in customer software development been analyzed for their security risks?					0
Do you have a security checklist for each OS deployed at your company?					0
Do you regularly perform audits (Internal or external) against your security checklists?					0
Are your system security checklists updated on a regular basis?					0
Are super user privileges regulated on systems in a written policy?					0
Are applications regulated from running as a super user privilege?					0
Do you require logon banners on systems ?					0
Are users with super user privileges reviewed and revised on a regular basis?					0
Do you have Anti-Virus software running on all of your Microsoft Platforms(Servers, Workstations, PC's and Laptops)?					0
Have you rolled out Anti-Virus Software to all of your email servers ?					0
Are all your Email servers configured to check all the incoming and outgoing emails for viruses, spams, trojan horses and other threats?					0
Do you have a procedure to ensure that all the servers, user machines, laptops are configured to automatically install the latest Virus Definition Files.					0
Do you have a mechanism in place to check all FTP inbound and outbound file transfers for viruses?					0
IDENTITY MANAGEMENT	**Response**	**"Yes" Details**	**Severity**	**Risk Score**	0
ACCOUNT MANAGEMENT (USER & HIGH PRIVILEGE ACCOUNTS)	**YES. NO. N/A.**	**Planned / just started. Partially completed. Fully implemented.**	**High. Medium. Low.**	**Calculated**	0
Is each customer account owned or sponsored by the customer ?					0
Does each account prohibit concurrent access (e.g. User cannot be logged in from two different machines)?					0
Are all user accounts deleted on the users' departure date?					0
Does the system disable user accounts after a period of inactivity?					0
Do you periodically reconcile system accounts to existing users?					0
Does the system lock user accounts after a number of failed attempts to login?					0
Do you have a consistent userid for a single person in all platforms & instances?					0
Are privileged accounts set up for emergency problem resolution fully logged and subjected to regular reviews ?					0
Do you have a policy on privileged accounts?					0
Do you have a compiled list of personnel with root or admin privileges?					0
Do you disable all the default account in all your server applications (e.g. Oracle's default DBA account and Oracle's default scott-tiger account, Windows default remote assistant accounts etc.) ?					0
PASSWORD MANAGEMENT AND AUTHENTICATION					0
Are users forced to change their passwords at first sign-on?					0
Do passwords expire periodically (e.g. every XX days)?					0

Are users prohibited from frequently re-using passwords (e.g. password can not be reused with in six months) ?					0
Do you periodically run password cracking software to identify weak passwords?					0
Do you have a process which notifies employees with weak passwords and forces a change?					0
Do you conduct internal audits to identify weak password using social engineering (e.g. password of a user is based on his son's name or the first word of the poster on his desk					0
EVENT MANAGEMENT	**Response**	**"Yes" Details**	**Severity**	**Risk Score**	0
EVENT MONITORING & INTRUSION DETECTION	**YES. NO. N/A.**	**Planned / just started. Partially completed. Fully implemented.**	**High. Medium. Low.**	**Calculated**	0
Is security auditing enabled on business critical systems (e.g. all servers configured to log any unsuccessful logn attempt etc.)?					0
Do you have a process to review security audit logs in a timely, consistent manner and act upon any threats identified by these reviews?					0
Is there an automated alerting/notification process that is initiated when defined security thresholds are exceeded?					0
Are you using network based Intrusion Detection (IDS) products on interconnections (e.g., Internet, web-hosting platforms, 3rd party connections)?					0
Do you periodically perform network penetration studies either using internal audits or through external consultants?					0
Is your business critical networks configured with Switches so that sniffer software is ineffective?					0
Is the intrusion detection system's network placement frequently reviewed to ensure appropriate coverage?					0
INCIDENT RESPONSE					0
Is there a process for users to report to IT when they have identified a potential virus on their system?					0
Do you have a documented Security Incident Response procedure?					0
Have you communicated the Security Incident Response procedure to all employees?					0
Do you conduct drills to verify the readiness of the company to any security incident?					0
DISASTER RECOVERY					0
Are there business mandated formal written Disaster Recovery Plans (DRPs) covering the partial or full loss of Servers, Critical Applications, Physical facilities ?					0
Are there disaster recovery facilities for critical systems located in a geographically independent area?					0
Have employees been trained on and are DRPs tested and updated on at least an annual basis?					0
Is there an owner responsible for devising and maintaining the DRPs ?					0
Have DRPs been reviewed and approved at the managerial level (e.g. by CIO)?					0
Have you identified “business critical” individuals to your business (i.e. how would you cope if 'x' left ?)					0
Has a business impact analysis been conducted on all customer applications and systems?					0

Have you identified and documented your business critical applications and applied Business Impact Analysis?					0
Are training sessions conducted for all relevant personnel on backup, recovery, and contingency operating procedures ?					0
ASSET SECURITY	**Response**	**"Yes" Details**	**Severity**	**Risk Score**	0
LAPTOP SECURITY	**YES. NO. N/A.**	**Planned / just started. Partially completed. Fully implemented.**	**High. Medium. Low.**	**Calculated**	0
Are all laptops required to be physically secured (e.g. cable lock) at all times?					0
Are users instructed to perform back ups on a regular basis on all laptops containing business and customer critical data?					0
Is there a process to ensure that business and customer critical data is encrypted?					0
Are employees who travel with laptops provided with theft prevention devices?					0
PHYSICAL SECURITY (BUILDINGS & CLIENT MACHINES)					0
Are ID badges issued to all working personnel (Permanent, contractor, agency temps,					0
Are personnel required to display their ID badges ?					0
Do ID badges have to be periodically renewed? (e.g. every 12 months)					0
Do you have visitor control procedures (i.e. are they logged in and out, and are they escorted within computer areas)?					0
Are fire detection / suppression systems required in your buildings?					0
Are your premises protected by intrusion detection systems e.g. CCTV ?					0
Do you require security guards on all of your sites keeping business and customer critical data ?					0
Do guards at entrances / exits randomly conduct spot checks to prevent unauthorized items from entering / leaving the building?					0
Are physical security breaches logged and investigated?					0
Are there random out of hours security inspections of the work place?					0
Are results of security inspections of the work place reported to senior management?					0
Is there a preventive maintenance program in effect for all environmental and protection systems?					0
PHYSICAL SECURITY (SERVER ROOMS)					0
Are firewalls kept in physically secure areas?					0
Is there a process to restrict access to computer centers only to people who have a business need?					0
Do you periodically review the list of people who have access to the computer center?					0
Do outside signs and building directories avoid making reference to computer centers or their locations ?					0
Are servers kept in protected areas with restricted access?					0
Are there established guidelines detailing what security is needed in areas where servers are (e.g. access control logs)?					0
ASSET INVENTORY					0
Do you have documented procedures for removing equipment from your facility?					0

Do you have an inventory of authorized modems and their phone numbers, and are these inventories regularly reviewed?					0
Is there a process in place to ensure that inventory for all computer equipment is maintained for accuracy and currency?					0
Do you have methods for the secure disposal of unwanted equipment and documents?					0
SOFTWARE MANAGEMENT					0
Is there a process to ensure software inventory is maintained for accuracy and currency?					0
Is license documentation physically available for review?					0
Are procedures in place to manage software license compliance?					0
Are new employees trained on the appropriate uses of company software?					0
Is an authorized software list maintained and users made aware of the fact that they can only install those applications that are included in this list ?					0
Are employees prohibited from installing unauthorized and pirated software on their desktop and laptop computers ?					0

TotalRisk Score	**17.5**
Maximum Possible Risk	**41**
%age risk abated:	**0.57317073**