Master Checklist

Auditing Entity-Level Controls

Checklist for Auditing Entity-Level Controls

□ 1. Review the overall IT organization structure to ensure that it provides for clear assignment of authority and responsibility over IT operations and that it provides for adequate segregation of duties.

□ 2. Review the IT strategic planning process to ensure that it aligns with business strategies. Evaluate the IT organization's processes for monitoring progress against the strategic plan.

□ 3. Determine whether technology and application strategies and roadmaps exist, and evaluate processes for long-range technical planning.

□ 4. Review performance indicators and measurements for IT. Ensure that processes and metrics are in place (and approved by key stakeholders) for measuring performance of day-to-day activities and for tracking performance against SLAs, budgets, and other operational requirements.

□ 5. Review the IT organization's process for approving and prioritizing new projects. Determine whether this process is adequate for ensuring that system acquisition and development projects cannot commence without approval. Ensure that management and key stakeholders review project status, schedule, and budget periodically throughout the life of significant projects.

□ 6. Evaluate standards for governing the execution of IT projects and for ensuring the quality of products developed or acquired by the IT organization. Determine how these standards are communicated and enforced.

□ 7. Ensure that IT security policies exist and provide adequate requirements for the security of the environment. Determine how those policies are communicated and how compliance is monitored and enforced.

□ 8. Review and evaluate risk-assessment processes in place for the IT organization.

□ 9. Review and evaluate processes for ensuring that IT employees at the company have the skills and knowledge necessary for performing their jobs.

□ 10. Review and evaluate policies and processes for assigning ownership of company data, classifying the data, protecting the data in accordance with their classification, and defining the data's life cycle.

□ 11. Ensure that effective processes exist for complying with applicable laws and regulations that affect IT (e.g., HIPAA, Sarbanes-Oxley) and for maintaining awareness of changes in the regulatory environment.

□ 12. Review and evaluate processes for ensuring that end users of the IT environment have the ability to report problems, have appropriate involvement in IT decisions, and are satisfied with the services provided by IT.

□ 13. Review and evaluate processes for managing third-party services, ensuring that their roles and responsibilities are clearly defined and monitoring their performance.

□ 14. Review and evaluate processes for controlling nonemployee logical access.

□ 15. Review and evaluate processes for ensuring that the company is in compliance with applicable software licenses.

Checklist for Auditing Entity-Level Controls (*continued*)

□ 16. Review and evaluate controls over remote access into the company's network (e.g., dial-up,VPN, dedicated external connections).

□ 17. Ensure that hiring and termination procedures are clear and comprehensive.

□ 18. Review and evaluate policies and procedures for controlling the procurement and movement of hardware.

□ 19. Ensure that system configurations are controlled with change management to avoid unnecessary system outages.

□ 20. Ensure that media transportation, storage, reuse, and disposal are addressed adequately by company-wide policies and procedures.

□ 21.Verify that capacity monitoring and planning are addressed adequately by company policies and procedures.

□ 22. Based on the structure of your company's IT organization and processes, identify and audit other entity-level IT processes.

Auditing Data Centers

Checklist for Auditing Data Centers

□ 1. Review data center exterior lighting, building orientation, signage, and neighborhood characteristics to identify facility related risks.

□ 2. Research the data center location for environmental hazards and to determine the distance to emergency services.

□ 3. Review exterior doors and walls to determine if they protect data centers facilities adequately.

□ 4. Evaluate physical authentication devices to determine if they are appropriate for the manner in which they are being used and are working properly.

□ 5. Review security guard building rounds logs and other documentation to evaluate the effectiveness of the security personnel function.

□ 6. Verify that sensitive areas are secured adequately.

□ 7. Verify that heating, ventilation, and air-conditioning systems maintain constant temperatures within the data center.

□ 8. Evaluate the data center's use of electronic shielding to verify that radio emissions do not affect computer systems or that system emissions cannot be used to gain unauthorized access to sensitive information.

□ 9. Determine whether the data center has redundant power feeds.

□ 10. Verify that ground to earth exists to protect computer systems.

□ 11. Ensure that power is conditioned to prevent data loss.

□ 12. Verify that battery backup systems are providing continuous power during momentary black-outs and brown-outs.

□ 13. Ensure that generators protect against prolonged power loss and are in good working condition.

□ 14. Ensure that a burglar alarm is protecting the data center from physical intrusion.

□ 15. Verify that a fire alarm is protecting the data center from the risk of fire.

□ 16. Ensure that a water alarm system is configured to detect water in high-risk areas of the data center.

□ 17. Ensure that a humidity alarm is configured to notify data center personnel of either high or low-humidity conditions.

□ 18. Review the alarm monitoring console(s) and alarm reports to verify that alarms are monitored continually by data center personnel.

□ 19. Ensure that data center building construction incorporates appropriate fire suppression features.

□ 20. Ensure that data center personnel are trained in hazardous materials handling and storage and that hazmat procedures are appropriate.

□ 21. Verify that fire extinguishers are placed every 50 ft within data center isles and are maintained properly.

□ 22. Ensure that fire suppression systems are protecting the data center from fire.

Checklist for Auditing Data Centers (*continued*)

□ 23.Verify that surveillance systems are designed and operating properly.

□ 24. Ensure that physical access control procedures are comprehensive and being followed by security staff.

□ 25. Review facility monitoring procedures to ensure that alarm conditions are addressed promptly.

□ 26.Verify that network, operating system, and application monitoring procedures provide adequate information to identify potential problems.

□ 27. Ensure that roles and responsibilities of data center personnel are clearly defined.

□ 28.Verify that duties and job functions of data center personnel are segregated appropriately.

□ 29. Ensure that emergency response procedures address reasonably anticipated threats.

□ 30.Verify that data center facility-based systems and equipment are maintained properly.

□ 31. Ensure that data center personnel are trained properly to perform their job functions.

□ 32. Ensure that data center capacity is planned to avoid unnecessary outages.

□ 33.Verify that procedures are present to ensure secure storage and disposal of system media.

Auditing Disaster Recovery

Checklist for Auditing Disaster Recovery

□ 1. Ensure that hardware redundancy is used to provide high availability where required.

□ 2.Verify that redundant systems at separate sites are used where very high system availability is required.

□ 3. Ensure that backup procedures are appropriate for respective systems.

□ 4.Verify that systems can be restored from backup media.

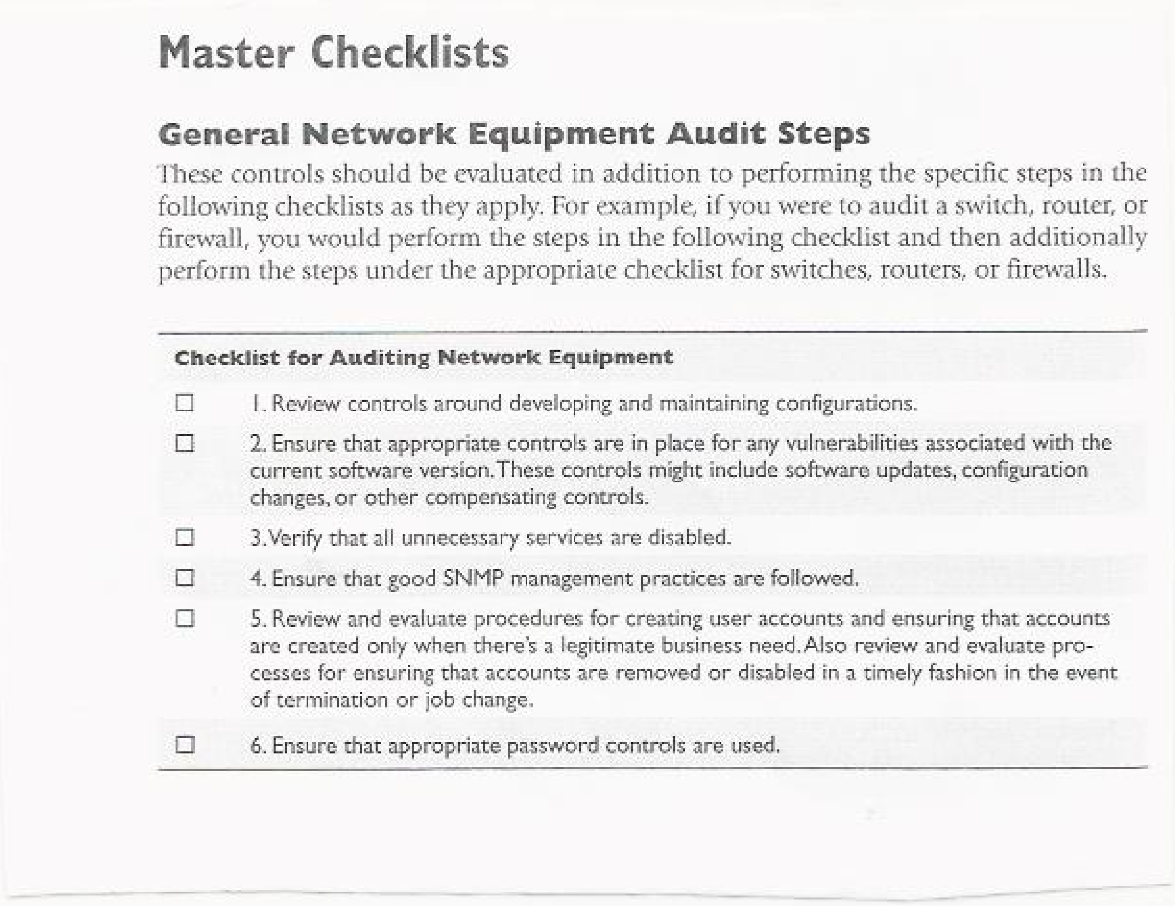
□ 5. Ensure that backup media can be retrieved promptly from off-site storage facilities.

□ 6. Ensure that a disaster recovery plan exists and is comprehensive and that key employees are aware of their roles in the event of a disaster.

□ 7. Ensure that disaster recovery plans are updated and tested regularly.

□ 8.Verify that parts inventories and vendor agreements are accurate and current.

□ 9. Ensure that emergency operations plans address various disaster scenarios adequately.



Master Checklists

General Network Equipment Audit Steps

These controls should be evaluated in addition to performing the specific steps in the following checklists as they apply. For example, if you were to audit a switch, router, or firewall, you would perform the steps in the following checklist and then additionally perform the steps under the appropriate checklist for switches, routers, or firewalls.

Checklist for Auditing Network Equipment

□ 1. Review controls around developing and maintaining configurations.

□ 2. Ensure that appropriate controls are in place for any vulnerabilities associated with the current software version. These controls might include software updates, configuration changes, or other compensating controls.

□ 3. Verify that all unnecessary services are disabled.

□ 4. Ensure that good SNMP management practices are followed.

□ 5. Review and evaluate procedures for creating user accounts and ensuring that accounts are created only when there's a legitimate business need. Also review and evaluate processes for ensuring that accounts are removed or disabled in a timely fashion in the event of termination or job change.

□ 6. Ensure that appropriate password controls are used.

Checklist for Auditing Network Equipment *(continued)*

□ 7.Verify that secure management protocols are used where possible.

□ 8. Ensure that current backups exist for configuration files if applicable.

□ 9.Verify that logging is enabled and sent to a centralized system.

□ 10. Evaluate use of the *Network Time Protocol* (NTP).

□ 11.Verify that a banner is configured to make all connecting users aware of the company's policy for use and monitoring.

□ 12. Ensure that access controls are applied to the console port.

□ 13. Ensure that all network equipment is stored in a secure location.

□ 14. Ensure that a standard naming convention is used for all devices.

□ 15.Verify that standard, documented processes exist for building network devices.

Auditing Layer 2 Devices: Additional Controls for Switches

These controls should be evaluated in addition to performing the general steps for auditing network equipment.

Checklist for Auditing Layer 2 Devices: Additional Controls for Switches

□ 1.Verify that administrators avoid using VLAN 1.

□ 2. Evaluate the use of trunk autonegotiation.

□ 3.Verify that Spanning-Tree Protocol attack mitigation is enabled (BPDU Guard, Root Guard).

□ 4. Evaluate the use of VLANs on the network.

□ 5. Disable all unused ports, and put them in an unused VLAN.

□ 6. Evaluate use of the *VLAN Trunking Protocol* (VTP) in the environment.

□ 7.Verify that thresholds exist that limit broadcast/multicast traffic on ports.

Auditing Layer 3 Devices: Additional Controls for Routers

These controls should be evaluated in addition to performing the general steps for auditing network equipment.

Checklist for Auditing Layer 3 Devices: Additional Controls for Routers

□ 1.Verify that inactive interfaces on the router are disabled.

□ 2. Ensure that the router is configured to save all core dumps.

□ 3.Verify that all routing updates are authenticated.

□ 4.Verify that IP source routing and IP directed broadcasts are disabled.

Auditing Firewalls: Additional Controls

These controls should be evaluated in addition to performing the general steps for auditing network equipment.

Checklist for Auditing Firewalls: Additional Controls

□ 1.Verify that all packets are denied by default.

□ 2. Ensure that inappropriate internal and external IP addresses are filtered.

Master Checklists

The following tables summarize the steps listed earlier for auditing Windows servers and clients.

Auditing Windows Servers

Checklist for Auditing Windows Servers

□ 1. Obtain the system information and service pack version, and compare with policy requirements.

□ 2. Determine if the server is running the company-provisioned firewall.

□ 3. Determine if the server is running a company-provisioned antivirus program.

□ 4. Ensure that all approved patches are installed per your server management policy.

□ 5. Determine if the server is running a company-provisioned patch-management solution.

□ 6. Review and verify startup information.

□ 7. Determine what services are enabled on the system and validate their necessity with the system administrator. For necessary services, review and evaluate procedures for assessing vulnerabilities associated with those services and keeping them patched.

□ 8. Ensure that only approved applications are installed on the system per your server management policy.

□ 9. Ensure that only approved scheduled tasks are running.

□ 10. Review and evaluate procedures for creating user accounts and ensuring that accounts are created only when there's a legitimate business need. Also review and evaluate processes for ensuring that accounts are removed or disabled in a timely fashion in the event of termination or job change.

□ 11. Ensure that all users are created at the domain level and clearly annotated in the active directory. Each user should trace to a specific employee or team.

□ 12. Review and evaluate the use of groups, and determine the restrictiveness of their use.

□ 13. Review and evaluate the strength of system passwords.

□ 14. Evaluate the use of password controls on the server, such as password aging, length, complexity, history, and lockout policies.

Checklist for Auditing Windows Servers (*continued*)

□ 15. Review and evaluate the use of user rights and security options assigned to the elements in the security policy settings.

□ 16. Review and evaluate the use and need for remote access, including RAS connections, FTP, Telnet, SSH, VPN, and other methods.

□ 17. Ensure that a legal warning banner is displayed when connecting to the system.

□ 18. Look for and evaluate the use of shares on the host.

□ 19. Ensure that the server has auditing enabled per your policies or organization's practices.

□ 20. Review and evaluate system administrator procedures for monitoring the state of security on the system.

□ 21. If you are auditing a larger environment (as opposed to one or two isolated systems), determine whether there is a standard build for new systems and whether that baseline has adequate security settings. Consider auditing a system freshly created from the baseline.

□ 22. Perform the steps from Chapter 4: Auditing Data Centers and Disaster Recovery as they pertain to the system you are auditing.

Auditing Windows Clients

Checklist for Auditing Windows Clients

□ 1. Determine if the client is running the company-provisioned firewall.

□ 2. Determine if the client is running a company-provisioned antivirus program.

□ 3. Determine if the client is running a company-provisioned patch-management solution.

□ 4. Determine if the client is equipped with the minimum recommended service pack, hotfixes, and software.

□ 5. Ensure that the client has all the following according to the *Microsoft Baseline Security Analyzer* (MBSA).

□ 6. Scan the system using a commercial-grade network scanner.

□ 7. Evaluate physical security controls during a walk-through.

Auditing Account Management and Password Controls

Checklist for Auditing Account Management and Password Controls

□ 1. Review and evaluate procedures for creating Unix or Linux user accounts and ensure that accounts are created only when there's a legitimate business need. Also review and evaluate processes for ensuring that accounts are removed or disabled in a timely fashion in the event of termination or job change.

□ 2. Ensure that all UID's in the password file(s) are unique.

□ 3. Ensure that passwords are shadowed and use strong hashes where possible.

□ 4. Evaluate the file permissions for the password and shadow password files.

□ 5. Review and evaluate the strength of system passwords.

□ 6. Evaluate the use of password controls such as aging.

Checklist for Auditing Account Management and Password Controls (*continued*)

□ 7. Review the process used by the system administrator(s) for setting initial passwords for new users and communicating those passwords.

□ 8. Ensure that each account is associated with and can be traced easily to a specific employee.

□ 9. Ensure that invalid shells have been placed on all disabled accounts.

□ 10. Review and evaluate super user (root-level) access.

□ 11. Review and evaluate the use of groups, and determine the restrictiveness of their use.

□ 12. Evaluate the use of passwords at the group level.

□ 13. Review and evaluate the security of directories in the default path used by the system administrator when adding new users. Evaluate the use of the "current directory" in the path.

□ 14. Review and evaluate the security of directories in root's path. Evaluate the use of the "current directory" in the path.

□ 15. Review and evaluate the security of user home directories and config files. They generally should be writable only by the owner.

Auditing File Security and Controls

Checklist for Auditing File Security and Controls

□ 16. Evaluate the file permissions for a judgmental sample of critical files and their related directories.

□ 17. Look for open directories (directories with permission set to `drwxrwxrwx`) on the system, and determine whether they should have the sticky bit set.

□ 18. Evaluate the security of all SUID files on the system, especially those that are SUID to "root."

□ 19. Review and evaluate security over the kernel.

□ 20. Ensure that all files have a legal owner in the `/etc/passwd` file.

□ 21. Ensure the `chown` command cannot be used by users to compromise user accounts.

□ 22. Obtain and evaluate the default umask value for the server.

□ 23. Examine the system's crontabs, especially root's, for unusual or suspicious entries.

□ 24. Review the security of the files referenced within crontab entries, particularly root's. Ensure that the entries refer to files that are owned by and writable only by the owner of the crontab. Also ensure that no crons are being run from open directories (permissions set to `drwxrwxrwx`).

□ 25. Examine the system's scheduled atjobs for unusual or suspicious entries.

Auditing Network Security and Controls

Checklist for Auditing Network Security and Controls

□ 26. Determine what network services are enabled on the system, and validate their necessity with the system administrator. For necessary services, review and evaluate procedures for assessing vulnerabilities associated with those services and keeping them patched.

□ 27. Execute a network vulnerability-scanning tool in order to check for current vulnerabilities in the environment.

□ 28. Review and evaluate the use of trusted access via the `/etc/hosts.equiv` file and user `.rhosts` files. Ensure that trusted access is not used or, if deemed to be absolutely necessary, is restricted to the extent possible.

□ 29. If anonymous FTP is enabled and genuinely needed, ensure that it is locked down properly.

□ 30. If NFS is enabled and genuinely needed, ensure that it is secured properly.

□ 31. Review for the use of secure protocols.

□ 32. Review and evaluate the use of `.netrc` files.

□ 33. Ensure that a legal warning banner is displayed when connecting to the system.

□ 34. Review and evaluate the use of modems on the server.

Auditing Audit Logs

Checklist for Auditing Audit Logs

□ 35. Review controls for preventing direct "root" logins.

□ 36. Review the `su` and `sudo` command logs to ensure that when these commands are used, they are logged with the date, time, and user who typed the command.

□ 37. Evaluate the `syslog` in order to ensure that adequate information is being captured.

□ 38. Evaluate the security and retention of the `wtmp` log, `sulog`, `syslog`, and any other relevant audit logs.

□ 39. Evaluate security over the `utmp` file.

Auditing Security Monitoring and Other Controls

Checklist for Auditing Security Monitoring and Other Controls

□ 40. Review and evaluate system administrator procedures for monitoring the state of security on the system.

□ 41. If you are auditing a larger Unix/Linux environment (as opposed to one or two isolated systems), determine whether there is a standard build for new systems and whether that baseline has adequate security settings. Consider auditing a system freshly created from the baseline.

□ 42. Perform steps from Chapter 4 as they pertain to the system you are auditing.

Master Checklists

Auditing Web Servers

Checklist for Auditing Web Servers

□ 1.Verify that the web server is running on a dedicated system and not in conjunction with other critical applications.

□ 2.Verify that the web server is fully patched and updated with the latest approved code.

□ 3. Determine if the web server should be running additional tools to aid in the protection of the web server.

□ 4.Verify that unnecessary services or modules are disabled. Running services and modules should be running with least privileged accounts.

□ 5.Verify that only appropriate protocols and ports are allowed to access the web server.

□ 6.Verify that accounts allowing access to the web server are managed appropriately and hardened with strong passwords.

□ 7. Ensure that appropriate controls exist for files, directories, and virtual directories.

□ 8. Ensure that the web server has appropriate logging enabled and secured.

□ 9. Ensure that script extensions are mapped appropriately.

□ 10.Verify that unnecessary or unused ISAPI filters are removed from the server.

□ 11.Verify the validity and use of any server certificates in use.

Auditing Web Applications

Checklist for Auditing Web Applications

□ 1.Verify that all input is validated prior to use by the web server.

□ 2.Verify that proper authorization controls are enforced.

□ 3. Broken authentication and session management

□ 4. Review the website for cross-site scripting vulnerabilities.

□ 5.Verify that the server is updated with all known patches for buffer overflows.

□ 6. Ensure that the web application is protected against injection attacks.

□ 7. Evaluate the use of proper error handling.

□ 8. Ensure that secure storage mechanisms are used correctly and appropriately.

□ 9. Determine the use of adequate controls to prevent denial of service.

□ 10. Review controls surrounding maintaining a secure configuration.

Master Checklist

Auditing Databases

Checklist for Auditing Databases

□ 1.Verify that database permissions are granted or revoked appropriately for the required level of authorization.

□ 2. Review database permissions granted to individuals instead of groups or roles.

□ 3. Ensure that database permissions are not implicitly granted incorrectly.

□ 4. Review dynamic SQL executed in stored procedures.

□ 5. Ensure that row-level access to table data is implemented properly.

□ 6. Revoke `PUBLIC` permissions where not needed.

□ 7. Restrict access to the operating system.

□ 8. Restrict permissions on the directory to which the database is installed.

□ 9. Restrict permissions on the registry keys used by the database.

□ 10. Check for default usernames and passwords.

□ 11. Check for easily guessed passwords.

□ 12. Check that password management capabilities are enabled.

□ 13. Check that auditing is enabled.

□ 14.Verify that network encryption is implemented.

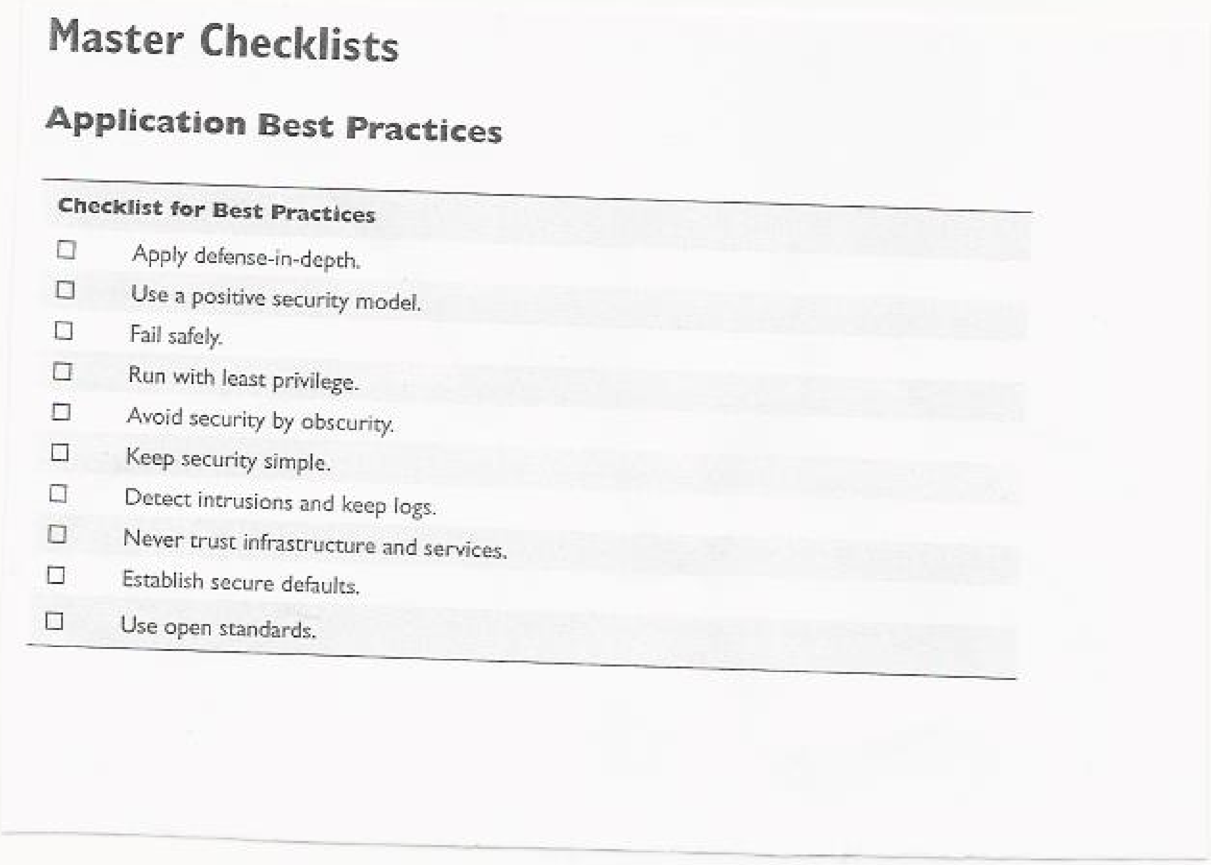
□ 15.Verify that encryption of data-at-rest is implemented where appropriate. Ensure that encryption key management is part of the disaster-recovery plan.

□ 16.Verify that the latest patches for the database have been installed.

□ 17.Verify that the database is running a version the vendor continues to support.

□ 18.Verify that policies and procedures are in place to identify when a patch is available and to apply the patch.

□ 19. Check the integrity of the database by looking for root kits, viruses, backdoors, and Trojan horses.



Master Checklists

Application Best Practices

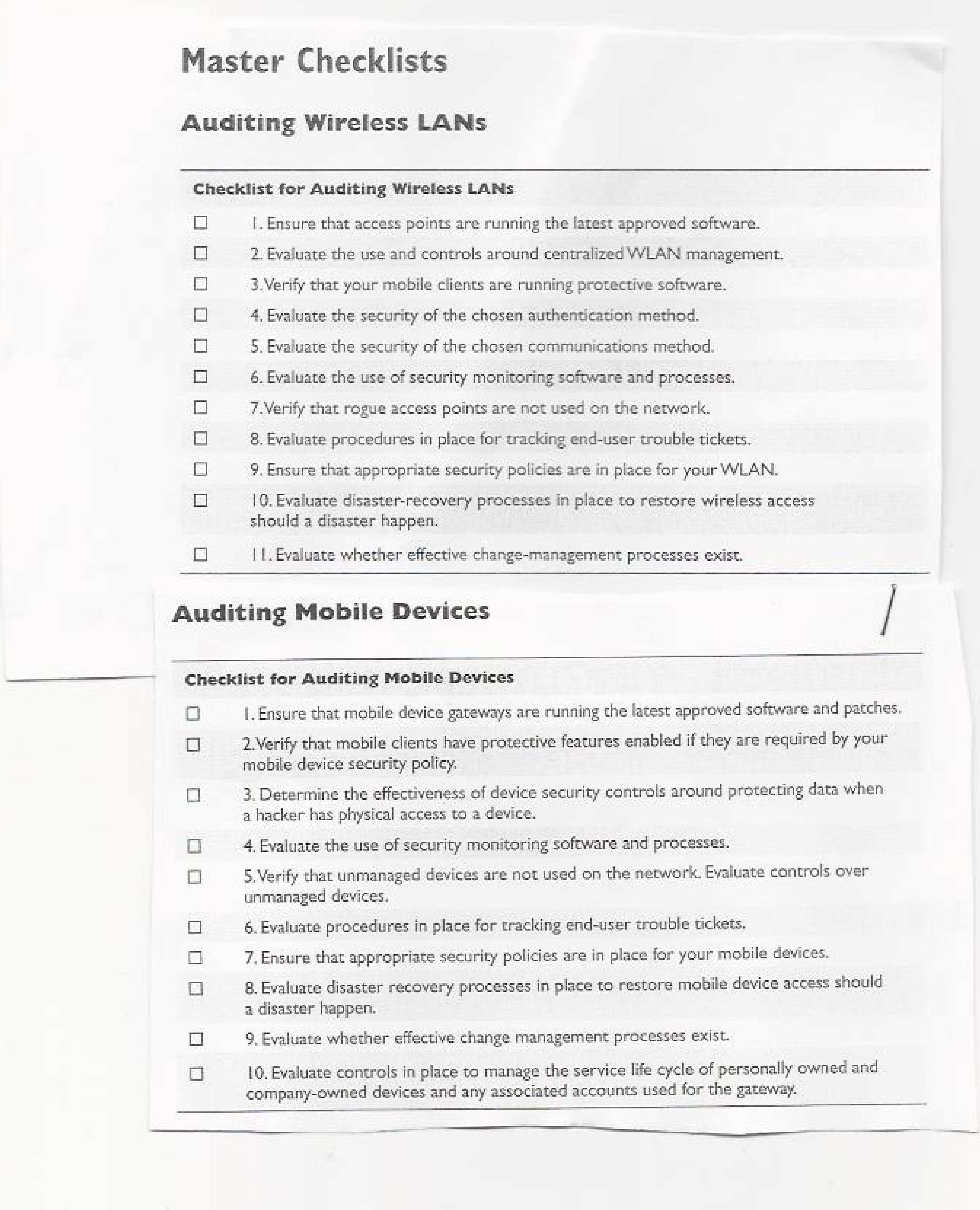
Checklist for Best Practices

- □ Apply defense-in-depth.
- □ Use a positive security model.
- □ Fail safely.
- □ Run with least privilege.
- □ Avoid security by obscurity.
- □ Keep security simple.
- □ Detect intrusions and keep logs.
- □ Never trust infrastructure and services.
- □ Establish secure defaults.
- □ Use open standards.

Auditing Applications

Checklist for Auditing Applications

- □ 1. Review and evaluate data input controls.
- □ 2. Determine the need for error/exception reports related to data integrity, and evaluate whether this need has been fulfilled.
- □ 3. Review and evaluate the controls in place over data feeds to and from interfacing systems.
- □ 4. In cases where the same data are kept in multiple databases and/or systems, periodic 'sync' processes should be executed to detect any inconsistencies in the data.
- □ 5. Review and evaluate the audit trails present in the system and the controls over those audit trails.
- □ 6. The system should provide a means to trace a transaction or piece of data from the beginning to the end of the process enabled by the system.
- □ 7. The application should provide a mechanism that authenticates users based, at a minimum, on a unique identifier for each user and a confidential password.
- □ 8. Review and evaluate the application's authorization mechanism to ensure that users are not allowed to access any sensitive transactions or data without first being authorized by the system's security mechanism.
- □ 9. Ensure that the system's security/authorization mechanism has an administrator function with appropriate controls and functionality.
- □ 10. Determine whether the security mechanism enables any applicable approval processes.
- □ 11. Ensure that a mechanism or process has been put in place that suspends user access on termination from the company or on a change of jobs within the company.
- □ 12. Verify that the application has appropriate password controls.
- □ 13. Review and evaluate processes for granting access to users. Ensure that access is granted only when there is a legitimate business need.
- □ 14. Ensure that users are automatically logged off from the application after a certain period of inactivity.
- □ 15. Evaluate the use of encryption techniques to protect application data.
- □ 16. Evaluate application developer access to alter production data.
- □ 17. Ensure that the application software cannot be changed without going through a standard checkout/staging/testing/approval process after it is placed into production.
- □ 18. Evaluate controls around code checkout, modification, and versioning.
- □ 19. Evaluate controls around the testing of application code before it is placed into a production environment.
- □ 20. Ensure that appropriate backup controls are in place.
- □ 21. Ensure that appropriate recovery controls are in place.
- □ 22. Evaluate controls around the application's data retention.
- □ 23. Evaluate controls around data classification within the application.



Master Checklists

Auditing Wireless LANs

Checklist for Auditing Wireless LANs

□ 1. Ensure that access points are running the latest approved software.

□ 2. Evaluate the use and controls around centralized WLAN management.

□ 3. Verify that your mobile clients are running protective software.

□ 4. Evaluate the security of the chosen authentication method.

□ 5. Evaluate the security of the chosen communications method.

□ 6. Evaluate the use of security monitoring software and processes.

□ 7. Verify that rogue access points are not used on the network.

□ 8. Evaluate procedures in place for tracking end-user trouble tickets.

□ 9. Ensure that appropriate security policies are in place for your WLAN.

□ 10. Evaluate disaster-recovery processes in place to restore wireless access should a disaster happen.

□ 11. Evaluate whether effective change-management processes exist.

Auditing Mobile Devices

Checklist for Auditing Mobile Devices

□ 1. Ensure that mobile device gateways are running the latest approved software and patches.

□ 2. Verify that mobile clients have protective features enabled if they are required by your mobile device security policy.

□ 3. Determine the effectiveness of device security controls around protecting data when a hacker has physical access to a device.

□ 4. Evaluate the use of security monitoring software and processes.

□ 5. Verify that unmanaged devices are not used on the network. Evaluate controls over unmanaged devices.

□ 6. Evaluate procedures in place for tracking end-user trouble tickets.

□ 7. Ensure that appropriate security policies are in place for your mobile devices.

□ 8. Evaluate disaster recovery processes in place to restore mobile device access should a disaster happen.

□ 9. Evaluate whether effective change management processes exist.

□ 10. Evaluate controls in place to manage the service life cycle of personally owned and company-owned devices and any associated accounts used for the gateway.

Master Checklists

Auditing Overall Project Management

Checklist for Auditing Overall Project Management

□ 1. Ensure that sufficient project documentation and software development process documentation (if applicable) have been created. Ensure that the company's project methodology standards are being followed.

□ 2. Review procedures for ensuring that project documentation is kept up-to-date.

□ 3. Evaluate security and change-management processes for critical project documentation.

□ 4. Evaluate procedures for backing up critical project software and documentation. Ensure that backups are stored offsite and that documented procedures exist for recovery.

□ 5. Ensure that an effective process exists for capturing project issues, escalating those issues as appropriate, and tracking them to resolution.

□ 6. Ensure that an effective process exists for capturing project change requests, prioritizing them, and dispositioning them.

□ 7.Verify that a project schedule has been created and that it contains sufficient detail based on the size of the project. Ensure that there is a process in place for monitoring progress and reporting significant delays.

□ 8. Ensure that there is a method for tracking project costs and reporting overruns. Ensure that all project costs, including labor, are considered and tracked.

□ 9. Evaluate the project leadership structure to ensure that both the business and IT are represented adequately.

Auditing Project Startup

Checklist for Auditing Project Startup

□ 10. Ensure that appropriate project approval processes were followed prior to project initiation.

□ 11. Ensure that a technical feasibility analysis has been performed along with, if applicable, a feasibility analysis by the company's legal department.

□ 12. Review and evaluate the requirements document. Determine if and how customer requirements for the project are obtained and documented before development takes place. Ensure that the customers sign off on the requirements and that the requirements encompass standard IT elements.

Checklist for Auditing Project Startup (*continued*)

□ 13. Evaluate the process for ensuring that all affected groups who will be helping to support the system, software, or process are involved in the project and will be part of the sign-off process, indicating their readiness to support it.

□ 14. Review the process for establishing the priority of requirements.

□ 15. Determine whether the system requirements and preliminary design ensure that appropriate internal control and security elements will be designed into the system, process, or software.

□ 16. If the project involves the purchase of software or technology, review and evaluate the vendor selection process and related contracts.

Auditing Detailed Design and System Development

Checklist for Auditing Detailed Design and System Development

□ 17. Ensure that all requirements can be mapped to a design element.

□ 18.Verify that the key stakeholders have signed off on the detailed design document (or equivalent).

□ 19. Review processes for ensuring ongoing customer involvement with the prioritization of tasks on the project.

□ 20. Look for evidence of peer reviews in design and development.

□ 21.Verify that appropriate internal controls and security have been designed into the system.

Auditing Testing

Checklist for Auditing Testing

□ 22.Verify that design and testing are taking place in a development/test environment and not in a production environment.

□ 23. Review and evaluate the testing process. Ensure that the project has an adequate test plan and follows this test plan.

□ 24. Ensure that all requirements can be mapped to a test case.

□ 25. Ensure that users are involved in testing and agree that the system meets requirements. This should include IT personnel who will be supporting the system and IT personnel who were involved in performing initial technical feasibility studies for the project.

□ 26. Consider participating in user acceptance testing and validating that system security and internal controls are functioning as intended.

Auditing Implementation

Checklist for Auditing Implementation

□ 27. Ensure that an effective process exists for recording, tracking, escalating, and resolving problems that arise after implementation.

□ 28. Review and evaluate the project's conversion plan. Ensure that the project has an adequate conversion plan and follows this plan.

□ 29. Review plans for converting the support of the new system or software from the project team to an operational support team.

□ 30. Ensure that sufficient documentation has been created for use of the system or process being developed and maintenance of the system or software. Evaluate processes for keeping the documentation up-to-date. Evaluate change controls and security over that documentation.

Auditing Training

Checklist for Auditing Training

□ 31. Review plans for making sure that all affected users are trained on the use of the new system, software, or process.

□ 32. Ensure that processes are in place for keeping training materials up-to-date. Evaluate change controls and security over the training materials.

Auditing Project Wrap-up

Checklist for Auditing Project Wrap-up

□ 33. Ensure that there is a process for closing out the project and recording lessons learned and that the process is followed.

EXAMPLE of a SECURITY AUDIT

SYNOPSIS

3. Recommendations

3.1. Physical accesses

The building seems to us suitably protected taking into account the activity of the Company. However, the access to the room server must be the subject of a detailed attention.

We recommend the installation of a data-processing room whose access should be restricted. Only authorized people should be able to intervene on the servers. This room must be suitably air-conditioned to ensure the correct operation of the material and to minimize the default risks.

3.2. Infrastructure

Although not having a direct relationship with security, we recommend the removal of the Sonicwall router. Indeed, it brings to the network a useless complexity increasing the default risk of the system.

Moreover that would allow the elimination of the non useful 192.128.1.0 /24 network which can prevent the access to certain Web sites.

A scheme of the simplified infrastructure is provided on the following page.

3.3. Internet Connections

As we saw, Internet connections present a good security. However, the type of distant control used by the Company is not recommended for the reasons clarified at the beginning of this document (Microsoft product) but also compared to the level of security reached.

Indeed, a robot can test from anywhere on Internet all the passwords to try to open a VPN tunnel and thus to be introduced on the server and the remainder of the network.

Two types of distant accesses are recommended depending on the situation:

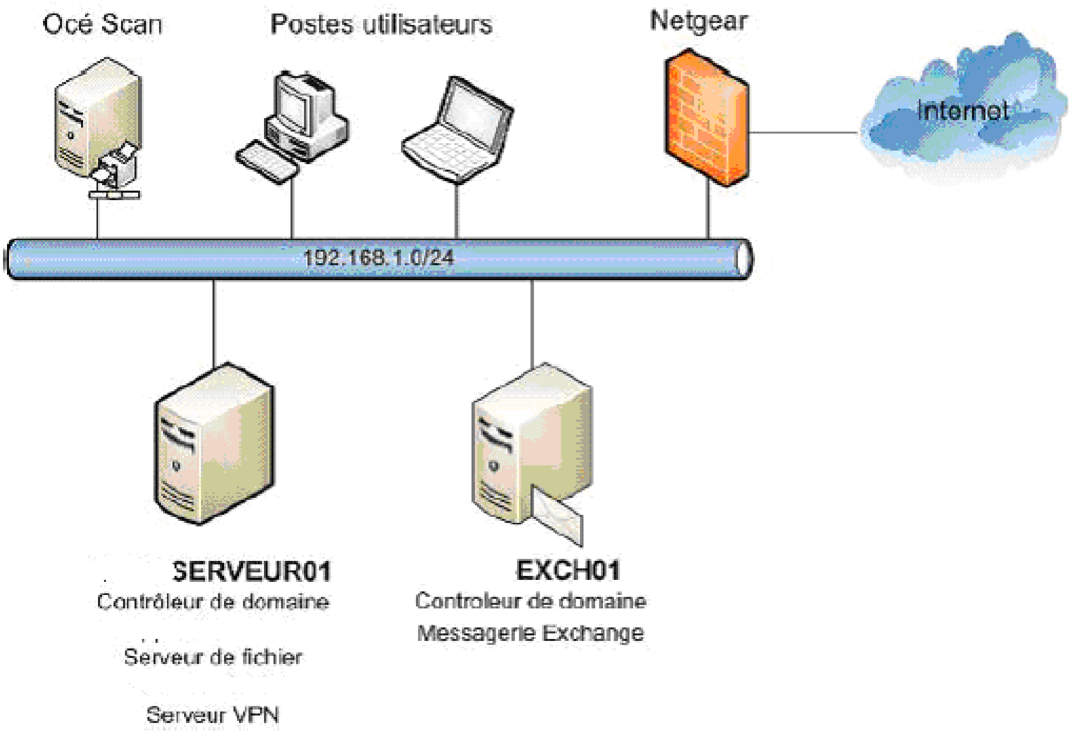
– places from where a distant access is desirable are well identified and have fixed public IP addresses,

– connections must be possible from anywhere on Internet.

In the first case, security must focus on the knowledge of a login/password (managed by Active Directory) and on the identification of the source. In fact the firewall must then be configured to filter the authorized sources from the non authorized ones.

In the second case, security must relate on the knowledge of a login/password and to the possession of a digital private key. Thus, the machines not having the certificate containing the private key do not have the possibility of establishing the link and cannot thus test logins/passwords.

We thus recommend the evolution of the remote control of the system used by the system administrator.



Scheme of the simplified infrastructure

3.4. Security of the client machines (machines)

In order to improve the security of the client machine, we recommend the following actions:

- assignment of a simple user rights for everybody in the company,
- reinforcement of the passwords strategy,
- installation of a WSUS update server,
- installation of a strategy of locking of accounts and sessions,
- installation of a firewall on each client machine.

3.4.1. Rights of the users

To remove the administrator rights for the personnel is the most important action to realize.

Indeed, when a person navigates on Internet, reads a virused e-mail or uses a USB key, it is better not to have the administrator rights in order to avoid the installation of a non desired malware. The installation of rootkits, Trojans, viruses, spywares and other malwares is then possible if the antivirus is not able to detect them or if the antivirus is disabled by the virus.

If the **user is not any more administrator of his machine**, the malware does not have any more the rights to allow its installation. Security is so reinforced, and the machines are better protected from the manipulation errors of the users.

If the Company wishes, as it is currently the case, to allow the users to install some software, or to modify for instance network parameters, it is possible to give them, in addition to their Active Directory account, a local administrator account on the machine.

3.4.2. Password strategy

We judge the **password strategy** in use a little too low, because the users tend to use too simple passwords.

We thus recommend the reinforcement of this strategy on the level of Active Directory by respecting the following constraints:
– password **with at least 8 characters**,
– at least 3 characteristics among the four following: **special characters, figures, small characters, capital characters,**
– validity of the password: 1 year,
– **only the user must know his password**. The administrator does not need to know it.
If a user loses her/his password, we recommend the following procedure:
– re-initialisation of the password with a default "one-time" password,
– then the user has to change the password at the first connection.

3.4.3. Installation of an update server

The system updates, currently, pose several problems:
– to follow-up updates,
– to control and guarantee their deployment,
– to avoid multiple remote loadings which can saturate the network, it is so better to manage these locally.
To answer these requirements, it is advised to use for instance a Windows WSUS **update server** which we recommend to install on a server. Its use by the client machines can be imposed via the "Windows Server" group strategies (GPO). Only one remote loading is then achieved and the follow-up of the updates is possible.

3.4.4. Locking of accounts and sessions

Automatic locking of sessions is useful to avoid the use of a machine by a non authorized person benefitting from the absence of the user. As the Company is not opened to the public and that the passage is restricted, a rather long time should not pose problems with the users while making it possible to ensure a sufficient level of security.
Concerning the locking of the accounts, it makes it possible to fight against the robots which would try to infiltrate on the network by testing many passwords (continuation for example to the installation of a Trojan horse on a machine customer).
We thus recommend for the Company, a **locking of the accounts at the end of 10 to 20 unfruitful attempts**. The administrator will be able to then unlock manually the account after having identified the cause of blocking.

3.4.5. Limitation of the access to Internet

Currently, the accesses to Internet are limited on certain machines by the application of a strategy forcing to go to internet through a proxy.
That is not sufficient because the installation of a different navigator (as Firefox) would allow navigation on Internet. Moreover, that by no means prevents the use of other tools (instantaneous message system, P2P, mailing...).
We thus recommend to allot a fixed IP to these machines (by reservations DHCP) and **to filter the access at the level of the firewall**. Indeed, located at this key point, security is more difficult to circumvent, especially if the user is not any more administrator of his machine.

3.5. Improvement of the procedures

3.5.1. Security charter

We strongly advise the **publishing of the security charter** on the use of computers and network. It makes it possible to the users to take note of the requirements of the Company and engages them with respect to the actions which they undertake.
Let us remind that the manager of the company and the head of the computing department are responsible for what the users do.

3.5.2. Activity continuity plan

We recommend the **installation of an activity continuity plan**. This will permit to anticipate possible crashes by thinking on the required strategies depending on the possible cases.

For the Company, it appears important to us to protect the company from the following risks:

- hardware crash of one of the two servers,
- hardware crash of the firewall,
- fire, flooding...

The evaluation of risks, as direct and hidden costs for the unavailability of the system would help to evaluate what is the best recovery solution which should be envisaged.

Recovery Tests would make it possible to check the correct operation of the saving systems.

4. Conclusion

The security installation of in the Company is overall good.

All the main elements are in operation and no major fault was detected.

A good base was fixed, but, as this audit shows it, many improvements are recommended.

With the evolution of the type of threats and vulnerabilities, it is important to permanently increase the level of security of the data-processing park. The achievement of the recommendations explained in this audit would make it possible to reach a more reassuring, more stable and more effective new threshold of security.