**The MPaudit : Questionnaire**

**Description**

Version of MPaudit questionnaire as at 17th Nov 2022

**Requirements**

Eyes

Answers

**The Process**

Get yourself an IUL, fill in the formstack version of the questionnaire, support will engage to kick off the audit

**How are known/unknown assets that connect to the organization's infrastructure documented, and how are unauthorized assets handled?**

Basic (1) No inventory of known assets. No action is taken on unauthorized assets.

Standardised (2) Company owned assets are registered and maintained in a central Configuration Management Database. No action is taken on unauthorized assets.

Rationalized (3) All company-owned asset information collection/update is automated and stored in the central Configuration Management Database for all available sources (e.g. mobile device manager and DHCP). Every week the process to check and either remove, deny or quarantine unauthorized assets is carried out.

Dynamic (4) All company-owned asset information collection/update is automated and stored in the central Configuration Management Database from all available sources (e.g. mobile device manager and DHCP). Unauthorized assets are detected and registered in the central Configuration Management Database automatically and classified as untrusted until asset is classified differently through the asset registration process.

**How are (software) applications identified and registered in your organisation?**

Basic (1) Applications are not being registered or managed.

Standardized (2) Application inventory is manual and unmanaged. A manual inventory process is in place to register applications. The process is unmanaged.

Rationalized (3) Application inventory is manual and managed. All applications are registered manually in the CMDB with information about ownership and lifecycle. Software cannot be released until it has been confirmed as registered in the CMDB. There is no insight in the use of unregistered software.

Dynamic (4) Application inventory is automated and managed. Applications are registered in the CMDB with appropriate information about ownership and lifecycle upon release. Application usage is monitored for both registered and unregistered (shadow-IT) software. Monthly reports on shadow-IT are provided to risk manager and/or security manager for further assessment.

**How do you ensure and check vendor supportability of used software and operating systems within the organization? How do you control non-approved software?**

"Basic (1) Unknown/unsupported and/or unwanted (cloud) software or operating systems are being used without documentation explaining (business justification) why that software is being used."

"Standardized (2) Unsupported and/or unwanted (cloud) software or operating systems are being used. Documentation with business justification is available per product, yet unmanaged. There is no insight where unsupported/unapproved software runs. No actions to mitigate the risks are in place."

"Rationalized (3) Unsupported and/or unwanted (cloud) software or operating systems are being used and documented programmatically. Mitigating controls and associated risks are managed. Unapproved software is manually deleted and replaced with authorized software."

"Dynamic (4) Unsupported and/or unwanted (cloud) software or operating systems are not used or are documented programmatically. Mitigating controls and associated risks are managed. Tools are in place to automatically discover, report, block and/or remove unauthorized software, based on business and risk management's decisions. Monthly compliance reports are sent to the stakeholders."

**How is data management organized in your organization?**

"Basic (1) Our organization does not have a data management policy. It is unclear where sensitive data resides or how data is protected."

"Standardized (2) A data management policy is available. Data management processes are implemented. There is no control regarding how the policies are being used."

"Rationalized (3) A data management policy is available. Data management processes are implemented. How data according to the policies is monitored, is in control for the majority of the organization. Business critical data is attack resilient. Data flows are not documented. Compliance is reported to stakeholders manually."

"Dynamic (4) A data management policy is available, and data management processes are implemented. Data flows are documented. Data compliance is monitored and automatically reported to stakeholders at least each quarter. Or organization has established attack resilient data management."

**How is access to data being controlled, how are checks being carried out on granted permissions?**

"Basic (1) Everyone has full access to all data in our organization."

"Standardized (2) Basic security groups have been implemented on shares, folders and collaboration sites/tools. We do not monitor given permissions."

"Rationalized (3) Role-based permissions have been implemented for all data resources. Permission changes are executed manually. Compliance reporting to stakeholders has not been implemented."

"Dynamic (4) Role-based permissions have been implemented to data resources based on least-privilege. Access is automatically granted/withdrawn based on the business roles matrix. Access auditing is implemented. Access attestation and report processes have been automated and sent to stakeholders to secure regulatory compliance."

**How is your data management process organized regarding data retention and secure data disposal?**

"Basic (1) A data retention and disposal process has not been implemented in our organization."

"Standardized (2) A data retention and disposal process has been established. The process is invoked manually."

"Rationalized (3) A data retention and disposal process has been implemented. The process is invoked automatically where this is supported. The process is reviewed annually. Compliance monitoring and reports have not been implemented."

"Dynamic (4) Data retention and disposal is implemented on all data resources. The enforcement of the policy is continuously monitored and can be assessed in a single report. Compliance reports are being sent to the respective stakeholders quarterly to prove compliance with the policy."

**What measures have been taken to store data at rest securely on devices and removable storage devices?**

"Basic (1) We have not implemented measures to secure data at rest on our devices."

"Standardized (2) Encryption is implemented on laptops, desktops and servers."

"Rationalized (3) Encryption is implemented on all devices, including smart phones, tablets, kiosks, cloud storage, USB storage etc.."

**How are secure configuration policies and security baselines (e.g. hardening) implemented in your organization?**

"Basic (1) Secure configuration policies and/or security baselines have not been implemented."

"Standardized (2) Secure configuration policies and/or security baselines are implemted only to Windows devices."

"Rationalized (3) Secure configuration policies and/or security baselines are implemented on all devices."

Dynamic (4) Secure configuration policies and/or security baselines have been implemented to all organizational devices. Devices are being continuously monitored for compliance, and are automatically denied access if a device is incompliant to the desired state.

**Has your organization implemented a policy to lock an idle device automatically?**

"Basic (1) A lock policy has not been implemented in our organization."

Standardized (2) A lock policy has been implemented only for servers, laptops, and desktops running Windows.

Rationalized (3) A lock policy has been implemented on all devices.

Dynamic (4) A lock policy has been implemented to all devices. Settings are enforced through centralized tools. If false unlock codes have been provided too many times, data is wiped. Compliance reports are sent monthly to the stakeholders, and incidents are alerted to the security team immediately.

**Have you deployed host-based firewalls to all systems that are able to have them? Are those firewalls configured to allow only inbound/outbound traffic for approved programs, protocols, network ports?**

"Basic (1) Host-based firewalls are not being used in our organization."

Standardized (2) The default firewall is enabled on all organizational devices. The settings and rules of the firewalls are not centrally managed.

Rationalized (3) Host-based firewalls are enabled and centrally managed on all devices that support it.

Dynamic (4) Host-based firewalls are implemented and centrally managed on all systems. Automated scans are performed to detect deviations to the policy. Conditional Access checks if the firewall is enabled as part of the risk assessment. Compliance reports are automatically sent to the stakeholders monthly.

**Are all default (admin) passwords for organizational assets, like applications, operating systems, printers, firewalls, and other (IoT) devices changed into unique passwords? Do the passwords used adhere to best practices?**

"Basic (1) There is no policy or process to change default (admin) passwords for organizational assets to unique passwords."

Standardized (2) A process has been implemented to change the default passwords of all devices/appliances that are being attached to our IT infrastructure.

Rationalized (3) Default passwords are changed for all devices/appliances before they are connected to the organizations infrastructure. Where possible the default usernames have been changed.

"Dynamic (4) Default passwords and usernames (if possible) are changed according to the process on all devices/appliances. These are stored in a central secure password vault. The network is monitored for network device vulnerabilities."

**Is there an inventory of all used accounts and how are dormant accounts handled?**

"Basic (1) Unknown or No inventory of the account information and no insight in dormant accounts."

"Standardized (2) Inventory of the account information is only available for administrator and service accounts, there is a manual process to check for dormant accounts."

"Rationalized (3) Inventory of the account information is available for all accounts including service accounts. There is a manual process scheduled to check for dormant accounts."

Dynamic (4) Inventory of the account information is available for all accounts including service accounts. There is an automated process scheduled to disabled dormant accounts with reporting to management

**How are the local administrator accounts managed?**

"Basic (1) Unknown or The local administrator accounts are not managed."

Standardized (2) The local administrator accounts have the same password on every machine.

Rationalized (3) All local administrator accounts have unique passwords or are disabled.

Dynamic (4) All local administrator accounts have either unique passwords or are disabled, and automated reporting is implemented for local administrator use

**How have you secured the privileged roles?**

Basic (1) Privileged roles are granted to normal user accounts.

Standardized (2) Privileged roles are granted only to dedicated admin accounts and are required to use Multifactor Authentication (MFA).

Rationalized (3) Privileged roles are granted only to dedicated administrator accounts and are required to use Multifactor Authentication (MFA). The administrator accounts can only be used on dedicated administrative devices and only at company approved locations.

Dynamic (4) Privileged roles are granted only to dedicated administrator accounts with JIT and are required to use Multifactor Authentication (MFA). The administrator accounts can only be used on administrative workstations. Accounts are monitored for suspicious behavior.

**Is account/identity management performed by the respective departments, with ownership of each identity, disabling dormant identities after a set period, and/or automatically expiring accounts?**

"Basic (1) No account management or ad hoc performed by IT."

"Standardized (2) Some accounts are checked by the business owner, but old/stale accounts are still lingering around."

"Rationalized (3) Most accounts are checked by the business owner, automatic expiration of old/unused accounts."

"Dynamic (4) All users are accounted for by the business, completely automated and regularly double checked by a functional owner."

**Do all (remote) access connections to the company systems and applications require the use of Multi Factor Authentication (MFA)?**

"Basic (1) Not defined/not implemented."

"Standardized (2) MFA is implemented to gain access to the company's (remote) systems and applications containing sensitive data. For the non MFA systems, long passwords/passphrases are implemented."

Rationalized (3) MFA is implemented for access to all the company's (remote) systems and applications. Including policies to enforce MFA for guest accounts.

Dynamic (4) MFA is implemented to gain access to all the company's (remote) systems and applications. Including policies to enforce MFA for guest accounts. A quarterly check is carried out to verify if the configured policies are up to date.

**Are there processes or tools in place to identify and remediate software or configuration vulnerabilities on the organization's systems?**

"Basic (1) No process available to identify or remediate software or configuration vulnerabilities."

Standardized (2) A manual process is available to identify or remediate software or configuration vulnerabilities. This process is performed on a quarterly, or more frequent, basis.

Rationalized (3) Automated vulnerability scans are executed using a SCAP-compliant vulnerability scanning tool on a quarterly, or more frequent, basis, to identify software or configuration vulnerabilities on the internal companies assets.

Dynamic (4) Automated vulnerability scans are done using a SCAP-compliant vulnerability scanning tool on a monthly, or more frequent, basis, to identify and remediate software or configuration vulnerabilities on the internal and external companies assets. Including reporting on anomalies.

**Has your organization implemented risk management processes to address: identification and classification of potential risks; mitigation controls (measures taken to reduce risk); acceptance/transfer of remaining (residual) risks after mitigation steps have been applied?**

"Basic (1) No risk assessments are performed."

"Standardized (2) Risk assessments are executed on ad-hoc basis. Risks are recorded in a register."

"Rationalized (3) Risk assessments are executed periodically. Risks are recorded in a register. Risk assessment methodology is reassessed on a periodic basis. "

Dynamic (4) Risk assessments are executed periodically. Risks assessment methodology is supported via automated tooling.

**Do you have an automated patch management solution implemented to continuously update all the organization's systems and applications?**

"Basic (1) Not implemented."

"Standardized (2) A manual patch management strategy for user endpoints and software is in place and executed monthly. Critical security hotfixes are applied as soon as possible."

Rationalized (3) An automated and scoped patch management strategy is in place and applied in a daily/weekly schedule. Critical security patches are applied immediately to core systems.

"Dynamic (4) An automated patch management strategy is in place for all user endpoint based on a monthly schedule. Critical security hotfixes are applied as soon as possible. Reporting and verification is carried out to ensure that all user endpoints are up-to-date. "

**Is there an audit log management process and how are the audit logs from the company devices (e.g. servers, network devices, command-line audit logs etc.) collected?**

"Basic (1) No audit log management process is available. Audit logs are not centrally collected."

Standardized (2) An audit log management process is available and the process is updated annually. Audit logs are not centrally collected.

Rationalized (3) An audit log management process is available and the process is updated annually. All audit logs are stored in a centralized location and retained for at least 90 days.

Dynamic (4) An audit log management process is available and scheduled. All audit logs are collected with detailed information to a centralized location and retained for at least 365 days.

**How are users prevented from installing unauthorized browsers, browser plugins, email client plugins, and add-on applications?**

"Basic (1) No restriction on the installation of browsers, browser plugins, email client plugins, and add-on applications."

Standardized (2) Users are made aware to not install unauthorized browsers, browser plugins, email client plugins, and add-on applications.

Rationalized (3) Tooling is used to ensure no unauthorized browsers, browser plugins, email client plugins, and add-on applications can be installed.

Dynamic (4) Tooling is used to ensure no unauthorized browsers, browser plugins, email client plugins, and add-on applications can be installed, with detection and reporting to management.

**Are network-based URL filters (incl. DNS filtering) implemented, limiting a system's ability to connect to unapproved websites?**

"Basic (1) Not implemented."

Standardized (2) URL, IP and DNS filters functionalities are being used, but not to the full extent of the IT infrastructure.

Rationalized (3) URL, IP and DNS filter functionalities are deployed to the full extent of the IT architecture.

Dynamic (4) URL, IP and DNS filter functionalities are deployed to the full extent of the IT architecture. Blocklist is regularly reviewed and updated.

**How have you setup the anti-malware solution on the company's assets?**

"Basic (1) Unknown/No central tooling is used."

Standardized (2) A centrally managed and enforced endpoint anti-malware solution is deployed to all company's servers and clients.

Rationalized (3) A centrally managed and enforced endpoint anti-malware solution is deployed to all endpoints (including mobile), all connected devices (USB also) are scanned. Where applicable, EDR functionality is enabled and configured.

Dynamic (4) A centrally managed anti-malware with EDR solution is deployed to all endpoints (including mobile); health states are monitored and alerts are forwarded to the designated team. Attack mitigation and remediation is automated and monitored by the team. Incident tickets are created automatically to minimize time between compromise and investigation/mitigation. Monthly reports are sent to stakeholders.

**How are autorun and autoplay configured on the company's systems?**

"Basic (1) Unknown/Autorun and autoplay features are enabled."

Standardized (2) Users are made aware to disable this functionality, users are able to edit the settings.

Rationalized (3) During deployment of the company's devices autorun and autoplay are disabled

Dynamic (4) Tooling is used to ensure the autoplay and autorun features are disabled and cannot be changed.

**How have you setup the data recovery process?**

"Basic (1) No data recovery process is available."

"Standardized (2) A data recovery process is available. Tooling is implemented to back-up the most important company's assets. Restore tests are only carried out when a restore is requested."

"Rationalized (3) A data recovery process is available. Tooling is implemented to back-up the all company's assets. Restore tests are carried out periodically as part of a structured process."

Dynamic (4) A data recovery process is available. Tooling is implemented to back-up the all company's assets and is resilient against datacenter failure. Each backup/system/application restore is tested and validated at least yearly. Compliance reports are sent to stakeholders.

**Are the backups encrypted and how are the backups stored?**

"Basic (1) Backups are not encrypted and only stored on-site"

Standardized (2) Backups are encrypted and stored only on-site.

"Rationalized (3) Backups are encrypted and an isolated instance of recovery data (e.g. Offline, off-site) and ransomware protection is applied."

Dynamic (4) Backups are encrypted and an isolated instance of recovery data (e.g. Offline, off-site), proof and reporting on all back-ups are sent to management

**What is the process to implement the latest stable version of any security-related updates on all network devices?**

"Basic (1) No process in place."

Standardized (2) A process is in place but is not scheduled or based on risks.

Rationalized (3) A process is in place and checks or updates are scheduled, no process for emergency patches.

Dynamic (4) A process is in place and checks or updates are executed regularly and whenever a new security patch version is available. The patch process is also risk based.

**Does your organization have a security and privacy awareness program?**

"Basic (1) No security and privacy awareness program is available."

Standardized (2) , A basic security and privacy awareness training is available to all employees.

Rationalized (3) An extended security and privacy awareness program is required for all employees.

Dynamic (4) An extensive privacy and security awareness program, including classroom and e-learning courses are required and scheduled for all employees (at least once a year).

**Is there a security awareness training program regarding secure logins, social engineering, sensitive data handling, unintentional data exposure, and reporting incidents?**

"Basic (1) No training program(s) available."

"Standardized (2) Basic training programs are available for some roles, covering some of the topics."

"Rationalized (3) Training programs are available for all organizational roles, on most topics."

"Dynamic (4) Training programs are available for all organizational roles, tailored, with measurements on the effect, and a specific focus for skills needed."

**How do you maintain an overview of the service providers used and what is the service providers management policy?**

"Basic (1) There is no overview of the service providers used."

tandardized (2) There is a list available with the used service providers, no process available for inventory of given access, assessment on security measures, monitoring, and decommissioning of the service providers.

Rationalized (3) There is a list available with the service providers used, A process is available for inventory of access granted, assessment of security measures, monitoring, and decommissioning of the service providers. The process is updated annually.

Dynamic (4) There is a list available of the service providers used. A process is available for inventory of access granted, assessment of security measures, monitoring, and decommissioning of the service providers. The process is scheduled with quarterly checks with reporting to management.

**Is an incident response (IR) procedure in place, covering reporting, data collection, management responsibilities, legal protocols and communication strategy?\***

"Basic (1) No procedure in place."

"Standardized (2) A basic incident response procedure is in place."

"Rationalized (3) A detailed incident response procedure with primary and secondary methods to report incidents is in place and includes staff roles, with regular drills."

"Dynamic (4) A detailed incident response procedure is in place, with periodic scenario based exercises. Post-incident reviews are executed regularly (including attack simulations at least once a year) and the organization is continually improving this process."