ISO 27001 Dashboard Compliance List

NO:	Dashboard Name	ISO 27001 Standard Control Number	Description
1	ISO-27001 -01- Account Management Summary	A.9.2.1	**User registration and de-registration:** A formal user registration and de-registration process shall be implemented to enable assignment of access rights.
		A.9.2.2	**User access provisioning:** A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services
2	ISO-27001 -02- Authentication Failure Summary	A.12.4.1	**Event logging:**Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.
		A.11.1.2	**Physical entry controls:** Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
3	ISO 27001 -03- Configuration or Policy Change Summary	A.14.2.2	**System change control procedures:** Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures
		A.12.1.2	**Change management:** Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.
		A.9.4.2	**Secure log-on procedures:** Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure
4	ISO-27001 -04- Disabled & Locked account summary	A.9.2.6	**Removal or adjustment of access rights:**The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change
		A.9.4.2	**Secure log-on procedures:** Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure
5	ISO 27001 -05- Enabled & Unlocked Account Summary	A.9.2.6	**Removal or adjustment of access rights:**The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change
		A.9.4.2	**Secure log-on procedures:** Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure

6	ISO27001 -06- File Integrity Monitor Log Summary	A.12.4.1	**Event logging:**Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.
		A.12.4.2	**Protection of log information:** Logging facilities and log information shall be protected against tampering and unauthorized access
		A.10.1	**Cryptographic controls:**To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information
7	ISO 27001 -07- Accounts Modification Summary	A.6.1.2	**Segregation of duties:** Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
8	ISO 27001 -08- Traffic to Internet Summary	A.13.2.1	**Information transfer policies and procedures:** Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities
		A.13.2.3	**Electronic messaging:** Information involved in electronic messaging shall be appropriately protected.
		A.14.1.2	**Securing application services on public networks:** Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification
		A.14.1.3	**Protecting application services transactions:** Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.
9	ISO 27001 -09- Traffic to Uncommon Ports Summary	A.14.1.3	**Protecting application services transactions:** Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.
10	ISO 27001 -10- Windows Firewall Change Summary	A.13.2.1	**Network controls:** Networks shall be managed and controlled to protect information in systems and applications.
		A.12.1.2	**Change management:** Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.

11	ISO 27001 -11- Applications Accessed By User Summary	A.9.4.1	**Information access restriction:** Access to information and application system functions shall be restricted in accordance with the access control policy
		A.9.4.4	**Use of privileged utility programs:** The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.
		A.11.2.7	**Secure disposal or reuse of equipment:** All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use
12	ISO 27001 -12- Uncommon softwares usage summary	A.12.6.2	**Restrictions on software installation:**Rules governing the installation of software by users shall be established and implemented.
		A.12.5.1	**Installation of software on operational systems:** Procedures shall be implemented to control the installation of software on operational systems.
13	ISO 27001 -13- File Monitoring Event-File Changes	A.12.4.1	**Event logging:** Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.
14	ISO 27001 -14- Use Of Non-Encrypted Protocols Summary	A.13.1.1	**Network controls:** Networks shall be managed and controlled to protect information in systems and applications.
15	ISO 27001 -15- Windows Host Configuration Change Summary	A.14.2.2	**System change control procedures:** Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures
		A.12.1.2	**Change management:** Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.
16	ISO 27001 -16- User Priv Escalation (SU & SUDO)	A.9.2.3	**Management of privileged access rights:** The allocation and use of privileged access rights shall be restricted and controlled.
		A.9.2.2	**User access provisioning:** A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services
17	ISO 27001 - 17 - Host Configuration Change Summary	A.14.2.2	**System change control procedures:** Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures
		A.12.1.2	**Change management:** Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.

18	ISO 27001 - 18 - Data Transfer Summary	A.13.2.1	**Network controls:** Networks shall be managed and controlled to protect information in systems and applications.
		A.13.2.2	**Security of network services:** Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced
		A.13.2.3	**Segregation in networks:** Groups of information services, users and information systems shall be segregated on networks
19	ISO 27001 - 19 - User Priv Escalation (Windows) Summary	A.9.2.3	**Management of privileged access rights:** The allocation and use of privileged access rights shall be restricted and controlled.
20	ISO 27001 - 20 - Software Installed Summary	A.12.5.1	**Installation of software on operational systems:** Procedures shall be implemented to control the installation of software on operational systems.
		A.12.6.2	**Restrictions on software installation:** Rules governing the installation of software by users shall be established and implemented
21	ISO 27001 - 21 - Software Uninstalled Summary	A.14.2.4	**Restrictions on changes to software packages:** Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.
		A.12.5	**Logging and monitoring:** To record events and generate evidence.
22	ISO 27001 - 22 - Remote Desktop Protocol Summary	A.13.1.1	**Network controls:** Networks shall be managed and controlled to protect information in systems and applications.
23	ISO 27001 - 23 - Monitoring Linux Processes	A.12.4.1	**Event logging:** Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.
24	ISO 27001 - 24 - Failed File System Access (Windows)	A.9.4.1	**Information access restriction:** Access to information and application system functions shall be restricted in accordance with the access control policy.
25	ISO 27001 - 25 - Audit Log Summary	A.12.4.1	**Event logging:** Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.
26	ISO 27001 - 26 - Detailed File Share Summary	A.9.4.1	**Information access restriction:** Access to information and application system functions shall be restricted in accordance with the access control policy.
27		A.13.1.1	**Network controls:** Networks shall be managed and controlled to protect information in systems and applications.

	ISO 27001 - 27 - Suspected Wireless Connection Attempt Summary	A.13.1.2	**Security of network services:**Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.
28	ISO 27001 - 28 - Critical Environment Error Summary	A.11.2.2	**Supporting utilities:** Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities
		A.12.4.1	**Event logging:** Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.
		A.14.2.6	**Secure development environment:** Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.
29	ISO 27001 - 29 - Failure Credential-validated Summary	A.12.4.1	**Event logging:** Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.
		A.9.2.4	**Management of secret authentication information of users:**The allocation of secret authentication information shall be controlled through a formal management process.
30	ISO 27001 - 30 - Social Media Summary	A.5.1.1	**Policies for information security:** A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties
31	ISO 27001 - 31 - Failed File System Access (Linux)	A.9.4.1	**Information access restriction:** Access to information and application system functions shall be restricted in accordance with the access control policy.
32	ISO 27001 - 32 - Rejected Connection to Network	A.13.1.1	**Network controls:** Networks shall be managed and controlled to protect information in systems and applications.
		A.9.1.2	**Access to networks and network services:** Users shall only be provided with access to the network and network services that they have been specifically authorized to use.
33	ISO 27001 - 33 - Detected Virus/Spyware Summary	A.12.2.1	**Controls against malware:** Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.
34	ISO 27001 - 34 -System File Permission Change (Linux)	A.9.4.1	**Information access restriction:** Access to information and application system functions shall be restricted in accordance with the access control policy.

35	ISO 27001 - 35 - Monitoring External Device Access	A.8.3.1	**Management of removable media:** Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization
		A.6.2.1	**Mobile device policy:** A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices
36	ISO 27001 - 36 - Detecting SSH Brute Force Attack Summary	A.11.1.4	**Protecting against external and environmental threats:** Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.
		A.9.4.2	**Secure log-on procedures:** Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure
		A.9.4.3	**Password management system:** Password management systems shall be interactive and shall ensure quality passwords.
37	ISO 27001 - 37 - Physical Security Summary	A.11.1.2	**Physical entry controls:** Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access
38	ISO 27001 - 38 - Unknown User Account Detail	A.9.2.5	**Review of user access rights:** Asset owners shall review users' access rights at regular intervals.
39	ISO 27001 - 39 - Time Sync Error Summary(Windows)	A.12.4.4	**Clock synchronisation:** The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source
40	ISO 27001- 40 -System Log File Deletion Summary (Linux)	A.12.4.2	**Protection of log information:** Logging facilities and log information shall be protected against tampering and unauthorized access.
		A.18.1.3	**Protection of records:** Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements
41	ISO 27001 - 41 - WebServer Access Logs Deleted Summary	A.12.4.2	**Protection of log information:** Logging facilities and log information shall be protected against tampering and unauthorized access.
		A.18.1.3	**Protection of records:** Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements