Internal Audit Division - ICT
Health Service Executive,
Bective Street, Kells, Co. Meath, A82 NX32.

Guidance for HSE Business Owners & Managers on Baseline IT Controls

March 2021

Table of Contents

1. Introduction

This Guidance for HSE Business Owners & Managers on Baseline IT Controls report provides a summary of common issues noted in ICT audits of HSE sites and the recommendations made to address these issues and control gaps.

This report has been developed jointly by the Internal Audit Division and the Office of the CIO (OoCIO) and will assist HSE Managers in guiding them to improve, where necessary, their IT control environment.

Internal Audit

The HSE's Internal Audit Division is responsible for ensuring that a comprehensive programme of audit work is carried out annually throughout the HSE. The purpose of this work is to provide assurance that controls and procedures are operated in accordance with best practice and with the appropriate regulations. The HSE Audit & Risk Committee monitors the work of the Internal Audit Division.

Office of the Chief Information Officer (OoCIO)

The Office of the Chief Information Officer (OoCIO) is responsible for the delivery of technology to support and improve healthcare in Ireland. The OoCIO is committed to realising the eHealth Ireland Strategy by ensuring that information and technology support healthcare efficiently and effectively throughout the whole health service. The purpose of the strategy is to provide an outline of eHealth and demonstrate how the individual citizen, the Irish healthcare delivery systems – both public and private – and the economy as a whole will benefit from eHealth.

2. Summary of Baseline ICT Controls

The table provided in Section 3 is categorised into the following areas:

- ICT Governance;
- Data Protection;
- Mobile Device Security;
- User Access Management;
- Third Party Access;
- Password Security;
- Application Security;
- Network Security;
- End-User Computing (EUC) Tools;
- Physical Security;
- System and Data Backups;
- ICT Helpdesk/Support;
- Integrated Patient Management System (IPMS).

3. Baseline IT Controls

This section provides a list of recommendations for IT controls. This list was compiled based on trends identified across a number of HSE sites. The baseline control objectives are categorised into control areas as described in Section 3 of this report.

3.1 ICT Governance

3.1.1 ICT Governance Structures:

Control Objectives
ICT governance structures and processes are implemented and championed by senior management.

Illustrative Control Activities
ICT governance can be embedded into existing management structures and forums such as the Executive Management Team (EMT) where the following occurs: • ICT is included as a scheduled agenda item on a regular basis; • Formal management reporting is carried out on key areas of ICT governance and management including ICT resource management, ICT performance management, ICT risks, ICT policies, ICT operations, and incidents; • Formal reporting covers all aspects of ICT, regardless of where devolved responsibility and management reside, for example in hospitals. It should cover technology elements managed by the ICT department as well as those managed elsewhere. At least, the following should be defined within the framework: • Assign responsibility for enforcing IT security; • Identify data owners and business owners for all key internal systems / applications; • Perform formal reviews on a regular basis of the level of access granted to sensitive data; • A data classification schema is introduced for the categorisation of data (e.g. sensitive, personal, HSE confidential, medical, etc.) and the level of protection required to protect the data is defined as per HSE policy, Information Classification & Handling Policy. See also HSE Data Protection Policy and related GDPR guidelines, and related policies listed at Appendix 4 of this document. • A proactive security management programme at an organisational level is defined (i.e. for the monitoring, testing and reporting of compliance against standards and policies); • Management are assigned responsibility for implementing policies and for reporting on ICT security policy compliance.

3.1.2 Roles & Responsibilities:

Control Objectives
Staff roles and responsibilities are defined. Specifically where ICT tasks may be administered by local, regional and/or national ICT teams.

Illustrative Control Activities
It is acknowledged that not every HSE site has dedicated ICT staff responsible for managing technical resources. Where this is the case, management still retain responsibility for the data they collect process and disclose. Formal communications and reporting should be agreed and implemented between senior management and the ICT custodians who are managing the data on their behalf. ICT custodians include: • Local ICT departments; • Local teams who manage end user applications/databases; • Regional / National ICT teams.

3.1.3 ICT Budgeting:

Control Objectives
Formal ICT Budgeting is conducted at local level and reported via the ICT governance structures.

Illustrative Control Activities
An ICT Budget has been prepared on the basis of existing commitments and known expenditure and includes at a minimum the following: • Contracts and commitments in place; • On-going maintenance; • Hardware and/or software upgrades; • Current projects. Management should ensure that all ICT expenditure items are accounted for under the ICT budget and formally reported as appropriate.

3.1.4 HSE ICT Security Policy Compliance

Control Objectives
The approved HSE suite of ICT security policies have been adopted and implemented. In addition, a compliance process that checks and reports on adherence is in place. Compliance reporting is embedded into the overall ICT governance process as a specific agenda item.

Illustrative Control Activities
The HSE national ICT security policies are implemented and a process to review and monitor compliance is in place. Management should consider implementing the policies most relevant to Data Protection as a matter of priority. These include: • Encryption Policy; • Access Control Policy; • Password Standards Policy; • HSE Data Protection Policy. Relevant Policies are listed at Appendix 4 in this document.

3.2 Data Protection

3.2.1 Training and Awareness:

Control Objectives
All staff collecting, processing and disclosing personal and sensitive data are made aware of their obligations under the General Data Protection Regulations (GDPR) and HSE Data Protection Policy. At a minimum, management responsible for the staff carrying out these tasks have been trained. It is recommended that all HSE staff undertake the HSELanD Data Protection training module. Specific reference is made in relation to manual and electronic data and the responsibilities that general staff and ICT have for processing, securing and backing up data.

Illustrative Control Activities
Management should ensure that all staff are made aware of their obligations in the collection, processing, securing and disclosure of personal and sensitive data. In addition: • In order to ensure that staff are both aware of their responsibilities under HSE Data Protection Policy and GDPR guidelines, and other organisational policies (see Appendix 4), the staff induction process includes data protection, organisational policy, how to recognise and how to report a breach; • For all HSE staff, a programme of data protection training is in place on HSELanD with particular emphasis on how to handle sensitive data; • Specific policies and guidance on the use of end user controlled systems has been developed and issued to all staff.

3.2.2 Secure File Transfer:

Control Objectives
The emailing of personal and sensitive data is prohibited. Where file transfer is required, the HSE site uses a facility to send data files in an encrypted format.

Illustrative Control Activities
Management have formally notified all staff that standard unencrypted email should never be used to transmit any data of a personal or sensitive nature, see also Encryption Policy and Electronic Communications Policy. Departments that wish to use email to transfer such data must ensure that personal or sensitive information is encrypted either through file encryption or through the use of a secure email facility that will encrypt the data (including any attachments) being sent.

Management have implemented a technical solution to allow transferred data to be encrypted.

3.3 Mobile Device Security

3.3.1 ICT Asset Register:

Control Objectives
A register of all ICT assets including laptops and other mobile devices is maintained by ICT. This asset register is used as a control to track and monitor laptops and ensure that they are encrypted.

Illustrative Control Activities
A register of all ICT assets including laptops should be maintained by local ICT. This asset register should be reviewed on a regular basis and used to track and monitor encrypted laptops. All HSE laptops are to be encrypted and included on the register and senior management are advised of the data protection risk via the ICT governance structures, HSE Encryption Policy and HSE Data Protection Policy.

3.3.2 Removable Media Devices:

Control Objectives
The use of removable media devices e.g. USBs on user PCs, is actively managed for all users.

Illustrative Control Activities
As per HSE Encryption Policy, all confidential and restricted information stored on removable storage devices must be encrypted. Confidential and restricted information may only be stored on HSE approved encrypted USB memory sticks where available from the OoCIO. The storage of confidential or restricted information on any other USB memory stick (encrypted or otherwise) will be considered a breach of policy. The following is a non-exhaustive list of USB devices that could be used to remove or copy personal / sensitive personal data: • External hard drive; • CD; • USB memory key; • iPod; • iPhone; • DVD.

3.3.3 Mobile Phone Security:

Control Objectives
All mobile devices must have disk encryption enabled. This includes mobile phones, especially where they are used to send and receive HSE emails.

Illustrative Control Activities
Management ensure that reviews are carried out on a regular basis of security policies implemented on central management servers, identifying all mobile email devices which have the capability to receive confidential or personal data via email and are provided to their staff. These reviews should ensure that content encryption is enabled on all mobile devices and should be enabled on standard mobile policy by default, Mobile Phone Device Policy refers.

3.4 User Access Management (Applies to Patient Management System, Network, VMWARE, Application and Databases)

3.4.1 New Joiners:

Control Objectives
New joiners are approved prior to being set up on the system.

Illustrative Control Activities
• A standard form / format is used to request and approve user access to the network and applications; • While the request can be made by the line manager, the access levels are approved by the system owner, or their delegated authority; • The principle of least access and segregation of duties is enforced; • Management retain evidence of the approval for staff joiners.

3.4.2 Privileged System Administration Access:

Control Objectives
Privileged levels of system administration access are restricted to a limited number of technical staff.

Illustrative Control Activities
• System default accounts are not used as generic accounts; • Individuals are assigned privileged access after formal approval is granted in order to create an audit trail; • Where privileged access is granted to a third party vendor, their access is restricted and managed; • The number of privileged or system administration users is kept to a minimum and granted only to those who are administering the system but not using it on a day to day or operational basis for operational purposes.

3.4.3 Generic Accounts:

Control Objectives
Generic accounts (i.e. accounts that are not specific to one named user) should not be created, and the use of any existing generic accounts to be reviewed at network and application levels.

Illustrative Control Activities
With the assistance of ICT, management review generic user accounts on the network domain and applications to determine if they are required. Unused or inactive generic accounts should be removed. In the event that the use of generic accounts is required, an exception request should be completed and approved. Responsibility for managing that generic account should be formally assigned to a single individual.

3.4.4 Movers Reviews:

Control Objectives
Staff mover access rights are modified on systems in a timely manner. Consideration is given to the old and new levels of access required by a user and the impact this may have on authority levels and segregation of duties.

Illustrative Control Activities

Management and/or HR should promptly notify ICT of the staff mover and date of moving; ICT modify the user accounts on the date that they are scheduled to change roles and confirm the actions taken with management who review for appropriateness.

3.4.5 Staff Leavers:

Control Objectives
Staff leavers are removed from systems in a timely manner.

Illustrative Control Activities
• Management and/or HR promptly notify ICT of the staff leaver; • ICT disable the user account on the date that the staff leaver is scheduled to leave; • Where contractors / third parties are granted access, a contract end date is set on the account to automatically disable it.

3.4.6 User Inactivity Reviews:

Control Objectives
Reviews of inactive user accounts on the local area network (LAN) and local applications including (but not limited to) the Patient Administration Systems (PAS) are conducted periodically.

Illustrative Control Activities
A list of user profiles is extracted from the system by ICT (or the system custodian) on a quarterly basis along with the last login date. Accounts that are inactive for 90 days, or more are disabled immediately.

3.5 Third Party Access (Applies to Network, VMWARE, Application and Databases)

3.5.1 Service Level Agreement(s) (SLAs):

Control Objectives
Service Level Agreement (SLA) is agreed between Third Party Service Provider(s) and the ICT department.

Illustrative Control Activities
• Service Level Agreements (SLA) are specific and define measurable target level or service such as uptime, response and resolution times; • SLAs are proactively monitored and their performance is periodically reported to management; • SLA should expressly require the third party and all its agents to comply with the provisions of HSE ICT policies; • SLA should include provision for the third party to provide assurance as to the secure processing and storage of said data in line with the requirements of GDPR; • Responsibilities of the third party in provision of services including regular extracting of data required for review purposes (for example audit logs, user access rights); • Responsibilities of the third party in safeguarding the security of data in line with GDPR; • Compliance with HSE policies; • Defined service levels based on requirements; • Mechanism for reporting on SLA compliance; • Penalties for non-compliance with service levels.

3.5.2 Access Rights:

Control Objectives
Access rights for Third Party contractors and vendors are restricted (not on an always on basis). Where privileged access is required for such third parties, additional compensating controls are in place.

Illustrative Control Activities
• Remote Access Policy is in place and applied by staff. • The level of access granted to Third Party service providers is regularly reviewed, documented, retained, and reassessed (e.g. every 3 months); • Third Party accounts are disabled when not required; they are only enabled for the time the access is required; • Where a Third Party needs to retain 24/7 access to the HSE internal resources (e.g. network, applications, databases, etc.), an automatic notification is implemented so that their activity is reviewed for appropriateness; • All key actions performed by the Third Party are logged, and the log is reviewed on a regular basis to identify inappropriate activity.

3.6 Password Security (Applies to Patient Management System, Network, VMWARE, Applications and Databases)

3.6.1 Password Configuration:

Control Objectives
All passwords must be a minimum of 8 characters in length and include a level of complexity, as per the HSE Password Standards Policy. These settings are enforced on all systems including the local area network (LAN) and all applications.

Illustrative Control Activities
Management ensure that the HSE Password Standards Policy is enforced on all systems. The policy includes, but is not limited to the following requirements: • All passwords must be a minimum of 8 characters in length; • Password complexity must be enabled - must contain a combination of letters (both upper & lower case), numbers (0-9) and at least one special character (for example: “, £, $, %, ^, &, *, @, #, ?, !, €); • Passwords must not be left blank; • A maximum password age of 90 days assigned for user accounts and a manual process for changing service account passwords on a periodic basis should be implemented.

3.6.2 Password Management:

Control Objectives
All passwords must be unique and known only to the user who is assigned the profile.

Illustrative Control Activities
Management ensure that the following practices are in place in line with the HSE Password Standards Policy and are enforced on the systems. • Users are forced to change their password on initial login; • Passwords are changed every 90 days; • No password should be re-used by a user within a 12 month period. • Passwords should not be written down by the security/system administrator; Where the above cannot be enforced on the system, management will raise a risk via the ICT governance process.

3.7 Application and Database Security (Applies to all applications including the Patient Management System and all local databases)

3.7.1 Service Catalogue:

Control Objectives
Management identify and formally document all applications / systems used within their respective HSE site into a service catalogue (i.e. a listing of those applications / systems with any relevant information including description, technology, data, etc.).

Illustrative Control Activities
The catalogue includes at a minimum the following information: • Business Owner; • System Administrator; • Sensitivity of the data held within the system.

3.7.2 User Activity Audit Logging:

Control Objectives
User activity logs are enabled at the application and database levels and reviewed on a regular basis. Audit logs are retained for potential future investigations.

Illustrative Control Activities
The following are applied at the application and database levels: • Auditing is enabled to include both successful and unsuccessful activity; • Privileged activity is recorded; • Log settings are configured to facilitate retention for at least 3 months. Management perform periodic reviews of user logs with a particular focus on privileged users.

3.7.3 Periodic User Access / Segregation of Duty Reviews

Control Objectives
Periodic review of access rights and segregation of duties are conducted on all applications including (but not limited to): • Patient Administration Systems; • Laboratory Systems; • Other systems / applications.

Illustrative Control Activities
A list of users for applications where sensitive / personal information is processed has been compiled in order to ensure a review is completed on all relevant systems. The following is completed on a periodic basis, depending on the sensitivity of the data: • User profiles with access to sensitive / personal / patient information are extracted by ICT (or the system custodian) from the application; • The information includes user name, role and access levels; • Management review the levels of access and check for appropriateness. • Consideration is given to segregation of duties and authority levels. Where patient data is processed on the application, the appropriateness of read only access is also assessed in line with GDPR.

3.7.4 Direct Access to Underlying Database(s):

Control Objectives
Direct access to databases containing personal, financial or sensitive data is restricted.

Illustrative Control Activities
Management review the access rights granted to all users on databases for appropriateness. Particular attention is given to privileged accounts. Accounts that are not required are promptly removed.

3.8 Network Security

3.8.1 User Activity Audit Logging:

Control Objectives
User activity logging is enabled on the network (including VMWARE) and reviewed on a regular basis. Audit logs are retained for potential future investigations.

Illustrative Control Activities
The following is applied at the network level on Active Directory: • At a minimum auditing is enabled to include both successful and unsuccessful activity across all network domains and on all elements of the global settings; • All privileged activity is recorded ; • Logs are retained for at least 3 months; • Management perform periodic reviews of user logs with particular focus on users with high privileges.

3.8.2 Periodic User Access / Network Share Reviews:

Control Objectives
Periodic reviews of access rights and segregation of duties are conducted on the network where personal and/or personal sensitive data is stored in an electronic format.

Illustrative Control Activities
Management with the assistance of ICT restrict access to network locations, shares, folders and files containing sensitive data to authorised users only. This access is granted in line with business roles and responsibilities, and is reviewed periodically.

3.8.3 Firewall Security:

Control Objectives
Appropriate levels of security are implemented on firewalls in respect to firewall rules, change control and logging.

Illustrative Control Activities
• Firewall rules are documented by ICT and description fields within the technical firewall rule set are completed for all rules; • An adequate level of change control is applied. At a minimum, ICT should assess the risk of each change and log all changes made to the system; • Firewall logs are reviewed by ICT on a periodic basis for inappropriate/unauthorised access attempts and irregular activity.

3.8.4 Intrusion Detection System (IDS):

Control Objectives
IDS is in place to monitor and detect irregular activity at the network perimeter.

Illustrative Control Activities
Management have defined which suspicious / dangerous network activities identified using the IDS should be actively monitored, by whom and how often. Where an IDS is not in place, management carry out a cost benefit analysis to determine if the risk of suspicious behaviour within their location justifies the financial expense. The results of this exercise should be escalated to the ICT governance structures.

3.8.5 Network Segmentation:

Control Objectives
Where appropriate, an adequate level of network segmentation is in place.

Illustrative Control Activities
Management ensure that access control mechanism are implemented to restrict access to authorised staff only, for at least the following key areas of the network: • Production servers; • Devices used for managing the virtual environment; • Storage Area Network devices.

3.8.6 Network Performance:

Control Objectives
Performance and capacity are monitored and the results are reported to support proactive network performance management.

Illustrative Control Activities
Network performance is monitored in real-time and thresholds have been defined for alerts to be triggered when they are exceeded. Network capacity is proactively managed and reported on to management on a periodic basis to prevent incidents occurring. Where the task of network performance is outsourced, management obtain regular reports providing positive assurance from the third party provider.

3.8.7 Anti-Virus Management:

Control Objectives
An antivirus solution is in place to protect all servers and desktops / laptops.

Illustrative Control Activities
Antivirus software is installed on servers and regularly updated to hold the latest signature file. Antivirus scans of the servers are configured to run at minimum on a weekly basis. Where more than one solution is in place, roles and responsibilities are formally documented and assigned for maintaining the antivirus solution (e.g. for ensuring that the antivirus is properly and regularly updated on all computers).

3.8.8 Security Patch Management:

Control Objectives
A process or automated tools for proactive patching of servers are in place.

Illustrative Control Activities
A patch management process is in place via a centralised management process. Patches are tested in a test environment prior to deployment into production, where possible. Management have developed and implemented ICT security standard documentation and supporting procedures that clearly define roles and responsibilities.

3.8.9 SAN & VMWARE Resilience:

Control Objectives
Management ensure that resilience is established for the key ICT resources including but not limited to Storage Area Network (SAN) and VMware.

Illustrative Control Activities
Management have reviewed their ICT resources and identified where key reliance is placed in order to ensure appropriate levels of resilience are in place. Specific consideration has been given to servers and data that are hosted on virtual environments and storage area network.

3.9 End User Computing (EUC) Tools (e.g. Microsoft Access Databases and Excel Spreadsheets)

3.9.1 Register of EUC Tools:

Control Objectives
All critical EUC tools are recorded and tracked.

Illustrative Control Activities
A register of all critical EUC tools is maintained. EUC tools that are used for the following should be considered critical: • To process personal or sensitive personal data; • Part of a business process and/or to perform critical financial calculations; • To provide important management information used for reporting and/or critical decision making.

3.9.2 EUC Security:

Control Objectives
All critical EUC tools are secured in accordance with HSE ICT policies and good practice for end user controlled databases.

Illustrative Control Activities
The owners responsible for the EUC tools ensure that the EUC tools are secured in accordance with HSE ICT policies and good practice for end user controlled databases. Specific control practices to note include: • The EUC tools are secured on the network and are backed up; • Access is restricted to the EUC tool on the network; • Password security is in place on the EUC tool; • Where possible segregation of duties is implemented; • Appropriate version control and archiving is in place; • Adequate documentation is in place explaining how the EUC tool is operated at a business process and ICT level.

3.10 Physical Security

3.10.1 Server Room:

Control Objectives
Servers hosting critical data are physically secured and access is restricted to technical staff who have a day to day business reason for accessing the servers.

Illustrative Control Activities
• All infrastructure is secured in a dedicated server room; • Access is restricted via an electronic key fob; • A list of authorised personnel has been approved and only technical staff with a day to day business reason are granted access; • All other staff or third parties who require access are granted on an as needs basis and a log of their visits is maintained; • Where access is not restricted by electronic key fob, management should consider compensating alternatives such as security cameras.

3.11 System and Data Backups

3.11.1 System and Data Backups:

Control Objectives
Management ensure that all systems and data are adequately backed up and that data is secure at all times.

Illustrative Control Activities
• Servers, applications and the data are backed up on daily, weekly/monthly or annual backups; • Back Up Tapes are encrypted and stored at a suitable offsite location; • Procedures are in place to secure the tapes and data. • Full restore testing is performed on a regular basis.

3.12 ICT Helpdesk / Support

3.12.1 Service Level Agreements (SLAs):

Control Objectives
SLAs are agreed between the business and the ICT department and ICT performance is measured against specific / defined targets.

Illustrative Control Activities
SLAs between the ICT Support Desk and the business teams are defined and agreed. These define the details of the technical support of critical systems and applications.

3.13 Patient Management System

3.13.1 Logical Access:

Control Objectives
User access is granted with adequate level of approval or authorisation and is periodically reviewed for appropriateness.

Illustrative Control Activities
• All user access is approved by the system owner before being granted; • The level of access granted must be commensurate with the user's job role; • Access rights are reviewed periodically and assessed against the user job role and the user's 'need to know'.

3.13.2 Privileged Access:

Control Objectives
All privileged access including system administrator and database administrator (DBA) accounts must be restricted to authorised personnel and based on their job role. This access must be periodically reviewed and monitored.

Illustrative Control Activities
• Privileged roles are restricted to a limited number of individuals who require the access for their daily job; • All privileged user accounts are reviewed periodically; • All privileged accounts' activity is logged, monitored and inappropriate activity is escalated and reported to management; • All privileged accounts are setup for named individuals; no generic accounts are allowed; • Privileged default system accounts are disabled or removed. Where this is not possible, these accounts' passwords are managed appropriately and their use is monitored.

3.13.3 Third Party Access:

Control Objectives
All third party access to the IPMS application and underlying database is authorised, restricted, reviewed and monitored.

Illustrative Control Activities
• Third party access to the IPMS application and database is restricted and is authorised by the system owner;

- Third party user accounts are reviewed periodically and promptly removed when the access is no longer required;
- All third party user access is monitored and periodically reviewed;
- Third party privileged access is only enabled for the duration of time the access is required.

3.13.4 Data Protection:

Control Objectives
Data held in the IPMS system is complete and up-to-date. All duplicates are removed promptly. Access to the data extracted from the system is protected and restricted to the same level as the data held within the system.

Illustrative Control Activities
• Data is periodically reviewed for completeness and accuracy; • Data is kept up-to-date and duplicate entries are promptly removed; • Access to extract data from the IPMS system is restricted; • All data extracted from the IPMS system can only be saved on restricted network shares that are monitored for access; • Read access to personal and sensitive data is logged and the logs are reviewed.

4. Appendix 1 – HSE Policies, Procedures & Guidelines

OoCIO Policies & Procedures Information is available at the following link:

http://hsenet.hse.ie/Intranet/OoCIO/

See also HSE IT Policies - Frequently Asked Questions here:-

http://hsenet.hse.ie/OoCIO/Service_Management/PoliciesProcedures/Policies/HSE_I_T_Policies_FAQ.pdf

General Data Protection Regulation (GDPR) Policies & Guidelines are available here:

http://hsenet.hse.ie/GDPR/