# ISO 27001 Statement of Applicability

| ISO27001: 2005 Ref. | ISO27001: 2013 ref | Section / Title | SPF Ref. v10 (new) | Progress | Evidence | Responsibility | Recommendations / Actions | Document name / location |
|---|---|---|---|---|---|---|---|---|
| A.5 | | **SECURITY POLICY** | | | | | | |
| A.5.1 | | **Information security policy** | | | | | | |
| A.5.1.1 | | Information security policy document | MR 4<br>MR 6 | Complete | Information Security Policy | InfoSec Mgr. | No action | Information Security Policy |
| A.5.1.2 | | Review of the information security policy | MR 4<br>MR 6 | Complete | Information Security Policy | InfoSec Mgr. | Yearly review | Document contained in the Corporate Document Centre (CDC). |
| **A.6** | | **ORGANISATIONAL AND INFORMATION SECURITY** | | | | | | |
| **A.6.1** | | **Internal organisation** | | | | | | |
| A.6.1.1 | | Management commitment to information security | MR 1<br>MR 2<br>MR 3 | Complete | Information Security Manager in post. The acceptance of implementing an Information Security Management System (ISMS) at board level. Documented in minutes of CLT meeting. | Corporate Leadership Team (Chief Fire Officer) | Ensure regular feedback to CLT via line manage and PSWG on implemented controls and further work needed to progress Information Security. | Statement of Applicability / PSWG SharePoint site. |
| A.6.1.2 | | Information security co-ordination | MR 1 | Complete | Information Security Manager in place.<br>Protective Security Working Group set-up. | InfoSec Mgr. | Protective Security Working Group established and a project to commenced to deal with the requirements of the Government Protective Security Strategy and Framework | |
| A.6.1.3 | | Allocation of information security responsibilities | MR 1<br>MR 6 | Complete | Information Security Manager in place. | InfoSec Mgr. | Allocation of Information Security responsibilities are outlined in the Statement of Applicability. | Information Security Manager Job Description and responsibilities. |
| A.6.1.4 | | Authorisation process for information | MR 8 | Complete | Authorisation will be from head of Corporate Planning and Intelligence Directorate and LT authorisation if applicable. | Head of Corporate Planning & Intelligence | Change management process and sign off by Head of CPI | |
| A.6.1.5 | | Confidentiality agreements | MR 9<br>MR 10<br>MR 11 | Complete | Employees required to adhere to confidentially requirements through published policies.<br>Confidentiality is standard clause for all company employees within their employment contract and third party agreements. | InfoSec Mgr. | **Confirm with all Directorates that they have either their own document or abide by the contract and terms of reference offered to the third party.**<br>**Documents will need to be entered into the CDC - not currently catalogued properly.** | |
| A.6.1.6 | | Contact with authorities | MR 12<br>MR 13 | Complete | a. Relevant contacts are in-place with authorities - specific to each directorate.<br>b. Security Incident procedures are in-place for contact with Internal audit team and the ICO. | InfoSec Mgr. | | |
| A.6.1.7 | | Contact with special interest groups | | Complete | a. iNetworks Knowledge Hub and NWARP (North West Warning, Advice and Reporting Point).<br>b. Regular communications with fire services and NWFC collaboration project. | InfoSec Mgr. | **Ensure that the ISM attends these quarterly meetings and pursues contact with other Fire Services.** | |
| A.6.1.8 | | Independent review of information security | MR 8 | Complete | Security consultancy - ECSC - review Jan 2012 and Aristi May 2013.<br>Recent vulnerability test took place on the internal network, wireless network and Mobile Data Terminals. | InfoSec Mgr. | Regular, on-going audits with Wigan Council Internal Audit Department and Audit Commission. | |
| A.6.2 | | **External parties** | | | | | | |
| A.6.2.1 | | Identification of risks related to external parties | MR 11 | Partial | a. Risks relating to third parties are to be added to the Risk Assessment Risk Register<br>b. Ensure that a list of external parties is kept up-to-date. | Each Directorate<br>&<br>SIRO | **- On-going - Risk assessments to be undertaken and Potential New Risks to be raised.**<br>**- Produce a list of all external parties and review regularly** | Directorate Risk Register |
| A.6.2.2 | | Addressing security when dealing with customers | MR 6<br>MR 10 | Partial | Risks relating to customers are to be added to the Risk Assessment. | Each Directorate | **A process is needed to record access by third parties.**<br>**Possible SharePoint site needed for recording access from external parties.** | Directorate Risk Register |
| A.6.2.3 | | Addressing security in third party agreements | MR 11 | Complete | Confidentiality and DPA is covered in standard contracts | Service Solicitor | Service Solicitor will keep this process up-to-date. | **Where is this recorded ?** |
| A.7 | | **ASSET MANAGEMENT** | | | | | | |
| A.7.1 | | **Responsibility for assets** | | | | | | |
| A.7.1.1 | | Inventory of assets | MR 7 | Partial | Asset Inventory held in SupportWorks, the ICT asset management / support desk system | ICT | Reports can be produced from the ICT SupportWorks system<br>**It is not however retrospective and there is no proven accuracy to historical data. This needs to be addressed.** | SupportWorks |
| A.7.1.2 | | Ownership of assets | MR 2 | Partial | a. Asset Inventory identifies user of equipment.<br>**b. Work is still being undertaken on identifying the Information Asset Owners.** | ICT<br>&<br>InfoSec Manager | a. Reports can be produced from the ICT SupportWorks system<br>**b. Produce an information Asset Register and train up Asset Owners.** | SupportWorks |
| A.7.1.3 | | Acceptable use of assets | MR 3 | Complete | Acceptable Use Policy | InfoSec Manager | Keep policy up-to-date on yearly review process. | Acceptable Use Policy |
| A.7.2 | | **Information classification** | | | | | | |
| A.7.2.1 | | Classification guidelines | MR 7 | Incomplete | Classification Scheme is not yet implemented. | Corporate Planning and Intelligence Dir. | Project to be initiated for this control, timescale not defined yet | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| A.7.2.2 | | Information labelling and handling | MR 7 | Incomplete | No Protective Marking scheme yet implemented. | Corporate Planning and Intelligence Dir. | Project to be initiated for this control, timescale not defined yet | |
| A.8 | | **HUMAN RESOURCES SECURITY** | | | | | | |
| A.8.1 | | **Prior to employment** | | | | | | |
| A.8.1.1 | | Roles and responsibilities | MR 1 | Complete | Roles for all employees are defined, including Information Security Manager. | People & Organisational Development | HR document / policy review process. To be included in the Corporate Document Centre. | |
| A.8.1.2 | | Screening | MR 13<br>MR 14 | Complete | All employees are screened for references, medical status, and where appropriate CRB.<br>Agency contract staff are not screened internally. | People & Organisational Development | HR document / policy review process. To be included in the Corporate Document Centre. | |
| A.8.1.3 | | Terms and conditions of employment | MR 11 | Complete | All employees are required to sign T&Cs | People & Organisational Development | HR document / policy review process. To be included in the Corporate Document Centre. | |
| A.8.2 | | **During employment** | | | | | | |
| A.8.2.1 | | Management responsibilities | MR 2 | Complete | Employees required to adhere to confidentiality requirements through published policies. | People & Organisational Development | Awareness of HR and Information security policies needed. | |
| A.8.2.2 | | Information security awareness, education and training | MR 3 | Partial | Training records are maintained for all employees by POD.<br>Formal Information Security Training not yet implemented. The Cabinet Office Awareness training modules are available but not yet implemented on GMFRS ICT systems. | ICT | A training structure is needed for Information Security awareness and Data Protection awareness. ICT to assess and implement the modules. | |
| A.8.2.3 | | Disciplinary process | MR 12 | Complete | Procedures and policies are in-place | People & Organisational Development | This process is included in HR and InfoSec Policies. | |
| A.8.3 | | **Termination or change of employment** | | | | | | |
| A.8.3.1 | | Termination responsibilities | | Complete | HR register leavers within POD iTrent system, which generates emails for the Line Manager and ICT. | People & Organisational Development / ICT | - Procedures should be defined to back up the process.<br>- Records should be kept and communication should be frequent between ICT and HR. | |
| A.8.3.2 | | Return of assets | | Complete | Line Manager is responsible for retrieving assets from leaver, as recorded in Asset Register. | People & Organisational Development / ICT | These should be kept up-to-date in the ICT SupportWorks system. | |
| A.8.3.3 | | Removal of access rights | | Complete | ICT Service Desk and Infrastructure team action account disabling and archiving for leavers. | ICT | Documented procedures needed | |
| A.9 | | **PHYSICAL AND ENVIRONMENTAL SECURITY** | | | | | | |
| A.9.1 | | **Secure areas** | | | | | | |
| A.9.1.1 | | Physical security perimeter | MR 18 | Complete | Perimeter is protected by gates, CCTV, and 24hr security guard on reception. | Finance and Technical Services | - CCTV procedures needed.<br>- Site Security audit to be completed | |
| A.9.1.2 | | Physical entry controls | MR 18 | Complete | Visitors are required to sign in. Staff and visitors have badges. Fobs required for access to specific areas. | Finance and Technical Services | Documentation / Procedures needed | |
| A.9.1.3 | | Securing offices, rooms and facilities | MR 17 | Complete | Entrance beyond reception requires fob access. Access is restricted in specific areas.<br>ICT and Finance departments are fob-controlled over-night.<br>Door-control system carries some risks – see Risk Assessment. | Finance and Technical Services | Documentation / Procedures needed | |
| A.9.1.4 | | Protecting against external and environmental threats | MR 18 | Complete | Environment is protected for smoke and fire. | Finance and Technical Services | Documentation / Procedures needed | |
| A.9.1.5 | | Working in secure areas | MR 18 | Complete | FSHQ Comms Rooms have secure entry procedures posted on doors. | Finance and Technical Services | Door notice and log book will need to be reviewed and updated if necessary on a yearly basis. | |
| A.9.1.6 | | Public access, delivery and loading areas | MR 18 | Complete | Deliveries restricted to reception and controlled by security. | Finance and Technical Services | Documentation / Procedures needed | |
| A.9.2 | | **Equipment security** | | | | | | |
| A.9.2.1 | | Equipment siting and protection | MR 17 | Complete | Data Centre has restricted access, and protection against fire, smoke and unauthorised access. Visitors to data centre must also sign-in. | ICT | Documentation / Procedures needed | |
| A.9.2.2 | | Supporting utilities | | Complete | Data Centre supported by UPS and cooling services. | ICT | Documentation / Procedures needed | |
| A.9.2.3 | | Cabling security | | Complete | Cabling is confined in trays, in structured cabling with walls/floors, or in patch cabinets. | ICT | Documentation / Procedures needed | |
| A.9.2.4 | | Equipment maintenance | | Partial | Equipment list should be held by the Estates Dept and the ICT Service Desk. This will be the asset register. All maintenance schedule should be held by these departments. | ICT | Documentation / Procedures needed | |
| A.9.2.5 | | Security of equipment off- premises | MR 9 | Partial | ########################################################################## | ICT | Documentation / Procedures needed | |
| A.9.2.6 | | Secure disposal or re- use of equipment | MR 9 | Partial | - If PCs are to be disposed or sold to third party reseller, ICT format all PC HDs with BLANCO - government specification formatting application.<br>- Contract for the disposal company is up for renewal, this has yet to be signed off (Sept 13) | ICT | PCs and Laptops are under this process. Printers and MFDs (Multi Function Devices) are under a contract with RICHO. Mobile phones need to be included in this clause. CCTV procedures to be identified. | |
| A.9.2.7 | | Removal of property | MR 9 | Partial | Removable Media and Mobile Device policy | ICT | Policy in place but no technical controls have been implemented. | Removable Media and Mobile Device Policy |
| A.10 | | **COMMUNICATIONS AND OPERATIONS MANAGEMENT** | | | | | | |
| A.10.1 | | **Operational procedures and responsibilities** | | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| A.10.1.1 | | Documented operating procedures | MR 10 | Partial | Some documented operating procedures | ICT | Not all operating procedures are documented or in a format to store centrally. This is being addressed with the Document Management System project and awareness training from the ISM. | |
| A.10.1.2 | | Change management | MR 8 | Partial | RFC process managed by ICT Service Desk Manager (Change Manager) and CAB meetings.<br>Not all changes are included in process – see Risk Assessment | ICT | All project that have an ICT involvement should follow this process, but it is not currently the way | |
| A.10.1.3 | | Segregation of duties | MR 8 | Incomplete | Rather than have segregation of duties, staff are trained in accordance with Data Protection guidelines and their obligations under their employment terms and conditions. | Information Security Manager / ICT | This will need to be assessed in relation to systems that store sensitive information and personally identifiable information. Personnel with extended ICT system access will need to be assed for segregation of duties. | |
| A.10.1.4 | | Separation of development, test and operational facilities | MR 8 | Partial | ICT staff have designated roles. Access privileges are assigned dependent upon their job requirements. | People & Organisational Development / ICT | Refer to the job descriptions and role requirements and departmental operating procedures. | |
| A.10.2 | | **Third party service delivery management** | | | | | | |
| A.10.2.1 | | Service delivery | MR 11 | Complete | Critical Suppliers are subject to SLAs, including C&W, Daisy | ICT | - A register of all SLAs with third party suppliers is needed. At present, Directorate Managers are in possession of these SLAs and there is no organisational wide register.<br>- Documentation and Register needed | |
| A.10.2.2 | | Monitoring and review of third party services | MR 11 | Complete | Regular Reports and service reviews for critical suppliers, including C&W, Daisy. | ICT | Documentation / Procedures needed | |
| A.10.2.3 | | Managing changes to third party services | MR 11 | Complete | Changes to Firewall configuration managed through Daisy change control.<br>Other supplier changes managed through internal RFC change process. | ICT | Documentation / Procedures needed | |
| A.10.3 | | **System planning and acceptance** | | | | | | |
| A.10.3.1 | | Capacity management | MR 8 | Complete | Network capacity monitored through Solarwinds, and contracted to Intrinsic. RFCs include requirement to identify capacity requirements for changes / installations. | ICT | Documentation / Procedures needed | |
| A.10.3.2 | | System acceptance | MR 8 | Incomplete | No formal Post Implementation Review (PIR) process in place. | ICT | Implement a Post Implementation Review | |
| A.10.4 | | **Protection against malicious and mobile code** | | | | | | |
| A.10.4.1 | | Controls against malicious code | MR 9 (GPG 7) | Complete | Antivirus installed on desktops, laptops and servers.<br>(CESG GPG 7: Protection from Malicious Code) | ICT | - Review needed on the administration and support of these solutions.<br>- Documentation / Procedures needed<br>- Patching Policy and Mobile Code Policy needed | Document contained in the Corporate Document Centre (CDC). |
| A.10.4.2 | | Controls against mobile code | MR 9 (GPG 7) | Complete | Antivirus installed on desktops, laptops and servers. | ICT | - Review needed on the administration and support of these solutions.<br>- Documentation / Procedures needed<br>- Patching Policy and Mobile Code Policy needed | Document contained in the Corporate Document Centre (CDC). |
| A.10.5 | | **Back-up** | | | | | | |
| A.10.5.1 | | Information back-up | MR 4 | Partial | - Back-up of servers is in operation.<br>- Off site back-up to Business Continuity site - Stretford Fire Station. | ICT | - Documentation of back-up process needed and procedures.<br>- List of all data that is backed-up and retention periods is needed.<br>- Schedule for the testing of backups is needed. | |
| A.10.6 | | **Network security management** | | | | | | |
| A.10.6.1 | | Network controls | MR 8 | Partial | Networks managed by dedicated ICT team.<br>Changes to the Network may be un-planned or outside ICT controls. | ICT | Change control process and procedures need to be confirmed. | |
| A.10.6.2 | | Security of network services | MR 9 | Partial | ICT approve changes to network security but third party is in control of the firewall and a number of systems on | ICT | - Contracts in-place with third parties for maintenance; contracts need to be entered into the CDC.<br>- Network security changes will be approved by ICT management and logged in the Support Works system.<br>- Procedures needed for all these processes | |
| A.10.7 | | **Media handling** | | | | | | |
| A.10.7.1 | | Network controls | MR 8 | Partial | - Policy on Removable Media and Mobile Devices published.<br>- There is no 'complete' technical control over removable media at this time (Sept. 13) | ICT | Implement an end point security solution. | Removable Media and Mobile Device Policy |
| A.10.7.2 | | Security of network services | MR 9 | Complete | Contract/Agreement for Waste Disposal | ICT | - Contract in-place for paper waste disposal with Shred-it.<br>- Agreement in-place for computer waste (hardware, peripherals and cabling) with Computer Waste Ltd | |
| A.10.7.3 | | Network controls | MR 8 | Partial | Information Security Policies are in-place but the technical controls need to be reviewed | ICT | Procedures needed for administering network access controls. | |
| A.10.7.4 | | Security of network services | MR 7 | Incomplete | Document Management System is in development | Corporate Planning and Intelligence Dir. | Information Management Strategy has been produced and the document management project is underway. | |
| A.10.8 | | **Exchanges of information** | | | | | | |
| A.10.8.1 | | Information exchange policies and procedures | MR 9 | Partial | Data Sharing Group set-up. No central repository of data sharing agreements has been produced.<br>Partnership Agreements are being implemented. | Data Sharing Group / Information Security Manager | The group meets every two months and TOR and minutes produced. The ISM is in the process of producing a GMFRS Data Sharing Agreement. | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| A.10.8.2 | | Exchange agreements | MR 9 | Partial | Central repository of agreements needed as they are currently held within the directorate that signs the agreement. | Corporate Planning and Intelligence Dir. | Organise the collation of all data sharing agreement needed within the CDC | |
| A.10.8.3 | | Physical media in transit | MR 7 | Partial | Removable Media and Mobile Device policy is in-place but technical controls need reviewing. | Information Security Manager | Organisational awareness needed for the policy.<br>Information Asset owners need training on transferring physical media. | |
| A.10.8.4 | | Electronic messaging | MR 7 | Partial | Acceptable Use Policy is in-place but technical controls need reviewing. | ICT | ISM to advise ICT on appropriate technical controls. | |
| A.10.8.5 | | Business information systems | MR 9 | Incomplete | Policy on connection with partners including Wigan MBC and NW RCC, not yet defined. | ICT | Confirmation of the systems required before we can confirm any contracts for SLAs in-place. ICT to supply the information. | |
| A.10.9 | | **Electronic commerce services** | | | | | | |
| A.10.9.1 | | Electronic commerce | | N/A | No online payment processing. | N/A | | |
| A.10.9.2 | | On-line transactions | | N/A | No online transaction processing. | N/A | | |
| A.10.9.3 | | Publicly available systems | | Complete | Website managed externally by Daisy (previously 2E2) with restricted access, under SLA and contract. | ICT | Need to supply evidence of the contract. | |
| A.10.10.1 | | **10.1 Monitoring** | | | | | | |
| A.10.10.1 | | Audit logging | MR 9<br>(GPG 13) | Complete | Windows domain event logging to Log Rhythm system.<br>Other servers and network devices not currently logged.<br>ICT implement SolarWinds and other logging systems. | Information Security Manager | Need to set-up review schedules for auditing. | |
| A.10.10.2 | | Monitoring system use | MR 9<br>(GPG 13) | Partial | Alerting and ad-hoc reporting from Log Rhythm on privileged account password changes, VPN access and large volume password changes.<br>Documented procedures not yet in place. | Information Security Manager | Documentation and scheduling needed. | |
| A.10.10.3 | | Protection of log information | MR 9<br>(GPG 13) | Complete | Access to Log Rhythm system is restricted to authorised users. | ICT | Procedures needed. | |
| A.10.10.4 | | Administrator and operator logs | MR 9<br>(GPG 13) | Complete | Admin and operator access is included in Windows event logs. | ICT | Procedures needed. | |
| A.10.10.5 | | Fault logging | MR 9<br>(GPG 13) | Complete | User and system fault reports and Service Desk actions are recording in Support Works. | ICT | Procedures needed. | |
| A.10.10.6 | | Clock synchronisation | MR 9<br>(GPG 13) | Complete | System automatically picks up clock synchronisation from Windows registered account. | ICT | Documentation needed. | |
| A.11 | | **ACCESS CONTROL** | | | | | | |
| A.11.1 | | **Business requirement for access control** | | | | | | |
| A.11.1.1 | | Access control policy | MR 10 | Complete | Access Control Policy produced. | Information Security Manager | | Access Control Policy |
| A.11.2 | | **User access management** | | | | | | |
| A.11.2.1 | | User registration | MR 9<br>MR 10 | Complete | New starters are added to AD by Service Desk following automatic notification from HR/Payroll System.<br>Removal of users through same channel, but ticket passes to Infrastructure team to archive data and remove account. | People & Organisational Development / ICT | Documentation / Procedures needed | |
| A.11.2.2 | | Privilege management | MR 9<br>MR 10 | Complete | Users are assigned departmental shares via Group Membership and deployed via login script. Additional share access is managed through ACLs and Groups, which are added to user as authorised by share owner. | People & Organisational Development / ICT | Documentation / Procedures needed | |
| A.11.2.3 | | User password management | MR 9<br>MR 10 | Complete | Password Guidance document. | Information Security Manager | | Password Guidance |
| A.11.2.4 | | Review of user access rights | MR 9<br>MR 10 | Incomplete | No review of user rights. | Information Security Manager / ICT | There is potential for users to retain inappropriate group membership when moving roles, and fob access to restricted areas.<br>The standard requires access reviews for all systems on a periodic, e.g. annual, basis. | |
| A.11.3 | | **User responsibilities** | | | | | | |
| A.11.3.1 | | Password use | MR 10 | Complete | Induction process advises that all staff read the Information Security Policies. | Information Security Manager | Annual review of policies and awareness training. | |
| A.11.3.2 | | Unattended user equipment | MR 10 | Complete | Clear Desk and Screen Policy. 10 minute screensaver enforced by AD Group Policy. | Information Security Manager | New staff are advised of policies in the induction process | |
| A.11.3.3 | | Clear desk and clear screen policy | MR 7<br>MR 10 | Complete | Clear Desk and Screen Policy. | Information Security Manager | Awareness training needs to be implemented. | |
| A.11.4 | | **11.4 Network access control** | | | | | | |
| A.11.4.1 | | Policy on use of network services | MR 7<br>MR 9 | Complete | Access control policy documented. ICT have process for assigning access privileges and recorded in the SupportWorks system. | ICT | | Access Control Policy |
| A.11.4.2 | | User authentication for external connections | MR 9 | Complete | 1. External users over the internet have VPN access with Vasco 2-factor authentication. | ICT | Administration documentation needed and yearly review schedule needed. | |
| A.11.4.3 | | Equipment identification in the network | MR 9 | Complete | 1. Internal wired network has Network Access Control (ForeScout) for device identification or authentication.<br>2. Internal wireless networks are restricted by MAC address authentication, WPA2/PSK security. | ICT | Administration documentation needed and yearly review schedule needed. | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| A.11.4.4 | | Remote diagnostic and configuration port protection | MR 9 | Complete | All network devices in secure comms rooms. | ICT | Network Access Control system needs to be fully implemented and reports to be reviewed regularly. | |
| A.11.4.5 | | Segregation in networks | MR 9 | Complete | Networks are segmented through routers and layer3 switches. | ICT | | |
| A.11.4.6 | | Network connection control | MR 9 | Partial | ################################################################## | ICT | Change Control process needs to be followed and properly documented.<br><br>Documentation / Procedures needed | |
| A.11.4.7 | | Network routing control | MR 9 | Complete | All routing managed by internal team for local and wide area networks. Connection to the internet managed by third party under SLA. | ICT | Intrinsic (third party) SLA and Documentation needed ... to be entered into the CDC. | |
| A.11.5 | | **Operating system access control** | | | | | | |
| A.11.5.1 | | Secure log-on procedure | MR 9 | Complete | Active Directory controls in-place. Domain Admin and priviledege access logons are requested via SupportWorks and authorised by ICT Manager. | ICT | The procedure needs to be documented and a review schedule set-up | |
| A.11.5.2 | | User identification and authentication | MR 9 | Partial | Users have unique Ids, but some historic use of shared Ids, which are still active. | ICT | The procedure needs to be documented and a review schedule set-up | |
| A.11.5.3 | | Password management system | MR 9 | Complete | This is in-place but it may be advisable to set the lock out procedure - Three wrong passwords and lock out for 5 mins | ICT | Advse ICT on the reasoning for the lock out process. | |
| A.11.5.4 | | Use of system utilities | MR 9 | Complete | Domain Administration is restricted to Infrastructure and Service Desk teams. | ICT | The procedure needs to be documented and a review schedule set-up | |
| A.11.5.5 | | Session time-out | MR 9 | Complete | 10 minute screen saver implemented on all systems. | ICT | The procedure needs to be documented and a review schedule set-up | |
| A.11.5.6 | | Limitation of connection time | MR 9 | Partial | There are limitations on connection time but this needs to be explored for individual systems | ICT | ICT to audit all systems and assess the need to impose time limitations on access. | |
| A.11.6 | | **Application and information access control** | | | | | | |
| A.11.6.1 | | Information access restriction | MR 9 | Incomplete | Information Asset Owner review currently being undertaken. | Information Security Manager / ICT | Information Asset review ids needed before allocation of access controls can be assigned.<br>Information Security Manager to assess Information Assets owners and ICT to implement controls | |
| A.11.6.2 | | Sensitive system isolation | MR 7 | Incomplete | Systems are in development (CRMS) that would hold sensitive information. | CPI / ICT | Project is already in-progress. Refer to the relevant CRMS project. | |
| A.11.7 | | **11.7 Mobile computing and teleworking** | | | | | | |
| A.11.7.1 | | Mobile computing and communications | MR 9 | Partial | Removable Media and Mobile Device policy in-place but there is no Teleworking or home working policy. | CPI / ICT | These policies need to be reviewed. The Information Management project will investigate how GMFRS staff will access and use information in the future. Project on-going | Removable Media and Mobile Device Policy |
| A.11.7.2 | | Teleworking | MR 9 | Incomplete | Removable Media and Mobile Device policy in-place but there is no Teleworking or home working policy. | POD / CPI / ICT | If this is to be progressed, then a project around home working needs to be created. This would involve ICT, POD and CPI. | |
| A.12 | | **INFORMATION SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE** | | | | | | |
| A.12.1 | | **Security requirements of information systems** | | | | | | |
| A.12.1.1 | | Security requirements analysis and specification | MR 16 | Partial | Where raised, RFCs include requirement to specify security controls.<br>Many changes are implemented without RFCs. | ICT | Change Management process needs to be properly implemented within the organisation. | |
| A.12.2 | | **Correct processing in applications** | | | | | | |
| A.12.2.1 | | Input data validation | | Incomplete | text to be completed ... | ICT | | |
| A.12.2.2 | | Control on internal processing | | Incomplete | text to be completed ... | ICT | | |
| A.12.2.3 | | Message integrity | | Incomplete | text to be completed ... | ICT | | |
| A.12.2.4 | | Output data validation | | Incomplete | text to be completed ... | ICT | | |
| A.12.3 | | **Cryptographic controls** | | | | | | |
| A.12.3.1 | | Policy on the use of cryptographic controls | MR 9 (HMG IAS 4) | Partial | BitLocker is deployed to all GMFRS PC laptops. There is key encryption but no documented proof of segregation of server and access controls. | ICT | Specify the process of storing encryption keys for BitLocker. | |
| A.12.3.2 | | Key management | MR 9 (HMG IAS 4) | Partial | Key management is in-place but needs to be documented | ICT | Documentation of procedures needed. | |
| A.12.4 | | **Security of system files** | | | | | | |
| A.12.4.1 | | Control of operational software | MR 9 | Incomplete | No documented process or procedures in-place. | ICT | Review of controls and documentation needed. | |
| A.12.4.2 | | Protection of system | MR 9 | incomplete | No documented process or procedures in-place. | ICT | Review of controls and documentation needed. | |
| A.12.4.3 | | Access control to program source code | MR 9 | Incomplete | No documented process or procedures in-place. | ICT | Review of controls and documentation needed. | |
| A.12.5 | | **Security in development and support processes** | | | | | | |
| A.12.5.1 | | Change control procedures | MR 8 | Partial | Formal RFC and CAB process managed through SupportWorks.<br>Not enforced for all changes. | ICT | Review of controls and documentation needed. | |
| A.12.5.2 | | Technical review of applications after operating system changes | MR 8 | Incomplete | No documented process or procedures in-place. | ICT | Review of controls and documentation needed. | |
| A.12.5.3 | | Restrictions on changes to software packages | MR 8 | Incomplete | No documented process or procedures in-place. | ICT | Review of controls and documentation needed. | |
| A.12.5.4 | | Information leakage | MR 7 | Incomplete | No documented process or procedures in-place. | ICT | Review of controls and documentation needed. | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| A.12.5.5 | | Outsourced software development | MR 9 | Incomplete | No documented process or procedures in-place. | ICT | Review of controls and documentation needed. | |
| A.12.6 | | **Technical vulnerability management** | | | | | | |
| A.12.6.1 | | Control of technical vulnerabilities | MR 8 | Partial | Desktops and laptops are managed for Microsoft updates via WSUS.<br>Servers are only patched at installation, to prevent conflict with applications.<br>Non-Microsoft product patches are only updated when upgraded. | ICT | A patch management solution and policy to be introduced | |
| A.13.1 | | **INFORMATION SECURITY INCIDENT MANAGEMENT** | | | | | | |
| A.13.1 | | **Reporting information security events and weaknesses** | | | | | | |
| A.13.1.1 | | Reporting information security events | MR 12 | Complete | Incident Policy. Incidents are recorded in Secure Works, for ICT events. Other security incidents not recorded. No definitive categorisation of events for ISM. | Information Security Manager | Policy has been updated.<br>The Service Desk should be updated on this policy and revised reporting procedure. | Security Incident Reporting Policy |
| A.13.1.2 | | Reporting security weaknesses | MR 12 | Partial | Incident Policy. Incidents are recorded in Secure Works, for ICT events. Other security incidents not recorded. No definitive categorisation of events for ISM. Reported to Head of CPI at weekly meeting and to CLT and LT. | Information Security Manager | Progress Information Security awareness within the organisation. | |
| A.13.2 | | **Management of information security incidents and improvements** | | | | | | |
| A.13.2.1 | | Responsibilities and procedures | MR 12 | Complete | Incident Policy has been adopted and all relevant departments and personnel are aware of their responsibilities. | Information Security Manager | Regular awareness training needed as part of the Information Security Group activities. | Security Incident Reporting Policy |
| A.13.2.2 | | Learning from information security incidents | MR 12 | Partial | Not fully implemented. Information Security Group needs to be set-up | Information Security Manager | Set-up the Information Security group | |
| A.13.2.3 | | Collection of evidence | MR 12 | Complete | Follow procedures as set-up in the policy and CESG guidance (HMG SPF) | Information Security Manager | HMG SPF guidance on security incidents to be implemented. | |
| A.14 | | **BUSINESS CONTINUITY MANAGEMENT** | | | | | | |
| A.14.1 | | **Information security aspects of business continuity management** | | | | | | |
| A.14.1.1 | | Including information security in the business continuity management process | MR 4 | Complete | Business Continuity management group co-ordinates Directorate Level BCPs. | Information Security Manager | The ISM is responsible for communicating information security issues with the Business Continuity Group. | |
| A.14.1.2 | | Business continuity and risk assessment | MR 4 | Complete | Each BCP has Business Impact Analysis to determine prioritisation for recovery of services with each Directorate. | Business Continuity Group | The ISM is responsible for communicating information security issues with the Business Continuity Group. | |
| A.14.1.3 | | Developing and implementing continuity plans including information security | MR 4 | Complete | Business Continuity Plans implemented for each Directorate. ICT Continuity Plan includes BCP site at Stretford. | Information Security Manager | The ISM is responsible for communicating information security issues with the Business Continuity Group. | |
| A.14.1.4 | | Business continuity planning framework | MR 4 | Complete | All Directorates complete BCP plans as part of the whole BCP for the Authority. BCP Review meetings held to co-ordinate plans and testing. | Business Continuity Group | The ISM is responsible for communicating information security issues with the Business Continuity Group. | |
| A.14.1.5 | | Testing, maintaining and re-assessing business continuity plans | MR 4 | Partial | Desktop testing of departmental tests, reviewed regularly.<br>Testing of BCP site not yet complete. | Business Continuity Group | ICT are due to go through testing on the BCS at Stretford S10 by the end of 2013. | |
| A.15 | | **BUSINESS CONTINUITY MANAGEMENT** | | | | | | |
| A.15.1 | | **Compliance with legal requirements** | | | | | | |
| A.15.1.1 | | Identification of applicable legislation | MR 6 (HMG IAS 5) | Complete | Authority receives many sources of advice on legislation, which are maintained through departments. Currently no central co-ordination of information security legislation. | Corporate Planning and Intelligence Dir. | Policy Officer now in-place within the CPI directorate. Communication with this post and the ISM who is chair of the GMFRS Protective Security Working Group means that all relevant legislation will be recorded and implemented in-line with our new project management methodology. | |
| A.15.1.2 | | Intellectual property rights (IPR) | MR 6 (HMG IAS 5) | Complete | IPR and copyright is maintained through contracts with third parties, in T&Cs of employment, and through control of installed software. | Deputy Clerk / Authority Solicitor | | |
| A.15.1.3 | | Protection of organisational records | MR 6 (HMG IAS 5) | Partial | Important HR and legal documents are kept under strict access control. Contracts may be held by departments, with no centralised record. | Corporate Planning and Intelligence Dir. | ########################################################## | |
| A.15.1.4 | | Data protection and privacy of personal information | MR 6 (HMG IAS 5) | Complete | Fully registered with the ICO for compliance with the DPA. | Corporate Planning and Intelligence Dir. | Data Protection Ofice and SIRO - Paul Sharples, Head of CPI. | |
| A.15.1.5 | | Prevention of misuse of information processing facilities | MR 6 (HMG IAS 5) | Complete | Acceptable Use Policy | Information Security Manager | | Acceptable Use Policy |
| A.15.1.6 | | Regulation of cryptographic controls | MR 6 (HMG IAS 5) | Partial | These needs covering in the Encryption Policy. | Information Security Manager | Encryption is standardised across the organisations laptops and there is an SFTP server in-place as well as secure email (.cjsm), But not documented<br>Produce an Encryption policy that incorporates laptops, Winzip, SFTP etc. | |
| A.15.2 | | **Compliance with security policies and standards and technical compliance** | | | | | | |
| A.15.2.1 | | Compliance with security policy and standards | MR 5 | Partial | Wigan MBC provide Internal Audit function for ICT. This does not cover all requirements for the standard. | ICT | Action the remaining recommendations within the agreed timescale.<br>Report to next Audit and Scrutiny Committee. | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| A.15.2.2 | | Technical compliance checking | MR 5 | Partial | Penetration Testing has been run historically. No recent scan. | ICT | Penn Test scheduled for Dec 2013. To include external firewall testing and wireless access.<br>MDT / airwave CoCo test to be arranged for Sept 2013. | |
| A.15.3 | | **Information systems audit considerations** | | | | | | |
| A.15.3.1 | | Information systems audit controls | MR 5 | Partial | Change management process is in-place but no evidence that this is followed as per ITIL recommendations. | ICT | The Change Management Board needs to be reintroduced to the organisation. | |
| A.15.3.2 | | Protection of information systems audit tools | MR 5 | Complete | Active Directory access controls are used and procedures for requesting access is through the ICT SupportWorks Help Desk system | ICT | Review schedule needs to be implemented. | |

| | |
|---|---|
| 39 | Partial |
| 71 | Complete |
| 21 | Incomplete |
| 2 | N/A |
| | |
| 133 | **Control Total** |

**GLOSSARY**

| | |
|---|---|
| ISM | Information Security Manager |
| CLT | Corporate Leadership Team |
| ICT | Information & Communications Technology |
| HIKM | Head of Intelligence & Knowledge Management |
| CPI | Corporate Planning and Intelligence Directorate |
| RM | Risk Manager |
| DC | Deputy Clerk and Authority Solicitor |
| POD | People and Organisational Development |
| BCG | Business Continuity Group. |
| | |