SCHEDULE OF SECURITY OBJECTIVES AND CONTROLS
INFORMAL ILLUSTRATION

Each "objective" and "essential outcome" should be mandatory, where applicable. The "measures and controls" should be implemented based on a risk assessment where appropriate to adequately address an information security risk, achieve the objective or essential outcome.

The purpose of this document is to give a flavour of how an IT professional or organisation might approach information security based on Annex A of ISO 27001. The idea is to give examples from high-level objectives to specific measures, but you may find that some categories overlap. The lists are not exhaustive.

The approach in this document is not exhaustive and it certainly does not represent the only or best approach to information security, which is a complex discipline. This document must not be relied on as advice and you should seek independent professional advice.

1. Information security policies

OBJECTIVE: Manage direction and support for information security to achieve the organisation's goals in compliance with applicable laws.

- **Essential outcomes**
  - Ensure board-level decision-making in relation to suitable IT assets, tools and technologies and the continuous support for their efficient, lawful and secure operation.
  - Implement a set of relevant information security policies mandatory for all personnel and relevant external parties.
  - Ensure regular review and board-level approval of the policies to ensure their continuous suitability, adequacy and effectiveness.
  - Dedicate adequate resources to information security.

2. Organisation of information security

OBJECTIVE: Establish a management framework to ensure the implementation and operation of adequate, documented and risk-based information security measures and controls within the organisation.

- **Essential outcomes**
  - Establish a hierarchy of personnel with assigned responsibilities in relation to information security, from senior executives such as CEO, CISO and CTO, as appropriate, to operational personnel.
  - Mitigate the risks of conflicting duties.
  - Implement information security governance policies and procedures, including risk assessment procedure.
  - Implement decisions based on risk assessment and legal and contractual requirements.
  - Monitor and measure compliance with policies and procedures through KPIs and enforcement.
  - Keep appropriate records and carry out regular audits, where appropriate.

- **Measures and controls**
- Periodically prepare an information security plan which is signed off by the board to address all risks.
- Carry out regular and comprehensive risk assessments to address each relevant information security risk followed by a documented decision on the measures and controls to be implemented to adequately mitigate such risk.
- Implement project management procedures to make information security integral in all stages of the project lifecycle and to adopt security by design and data protection by design and default, where appropriate.
- Monitor all relevant public vulnerability reporting channels.
- Establish communication channels between the IT department and personnel and encourage reporting.
- Engage in awareness-raising and provide appropriate training to all personnel, as appropriate.

3. Mobile devices and teleworking

OBJECTIVE: Establish a management framework to ensure the security of teleworking and the use of mobile devices.

- **Essential outcomes**
  - Implement mobile device policy, bring your own device (BYOD) policy, and teleworking policy, as appropriate.
  - Implement defence-in-depth strategy in relation to valuable information assets, where appropriate.
  - Provide user training.
  - Monitor adherence to policies and procedures.

- Measures and controls
- Implement measures and controls to address registration and management, physical protection, app whitelisting (AWL), patch management, define what information is accessible and, where appropriate, restrict access to critical assets, cryptography, malware and antivirus, log on, remote disabling, erasure, lockout and 'find my device' requirements, backup and storage, family user access conditions e.g. separation of accounts, use in public places, connectivity and trusted networks, training and audits.

4. Human resource security

OBJECTIVE: Ensure employees and contractors understand their information security responsibilities corresponding to their roles from the start of their engagement and protect the organisation's interests when terminating engagements.

- **Essential outcomes**
  - Implement HR controls to mitigate accidental or malicious threats.
  - Engage managers to play their role in developing a security culture by raising awareness, ensuring policy adoption by personnel, and reinforcing the contractual obligations of personnel.
  - Provide training and raise awareness about responsibilities, policies and procedures as well as threats, vulnerabilities and controls.
  - Implement orderly leaver process.

- Measures and controls
- Screen personnel for background and competence, as appropriate, in accordance with applicable laws.
- Enter into appropriate contracts with personnel covering information security obligations, confidentiality, acceptable use, ownership of intellectual property, return of assets and other matters.
- Reinforce obligations of leavers and personnel moving to new roles.
- Assign roles on the basis of reliability, experience and technical abilities.
- Provide mandatory information security training appropriate to role and access privileges.
- Evaluate adherence to policies and procedures during HR personnel reviews.
- Ensure personnel understand their obligation to lock away equipment and documents overnight in secure cabinets, securely dispose of any confidential printouts, not leave documents on printer, not keep post-it notes with confidential information in sight, not share login details, not store confidential information on unprotected portable devices, not open suspicious emails, and other essential security obligations.
- Invoke disciplinary process in case of failure to comply.

5. Information asset management and media

OBJECTIVE: Classify information assets, define appropriate level of protection and prevent unauthorised disclosure, modification, removal or destruction of information stored on media.

- **Essential outcomes**
  - Maintain an inventory of information assets.
  - Ensure consistent labelling of information assets.
  - Implement acceptable use policy.
  - Securely dispose of information assets.

- Measures and controls
- Carry out data mapping and keep appropriate records.

- ○ Implement acceptable use policy to address appropriate use of IT resources, access controls, the responsibilities of information asset owners, security of physical media transfers, confidentiality, intellectual property, contractual obligations, regulatory responsibilities, data sharing, return of assets, private use, and to encourage conduct that preserves security.
- ○ Design personal data fields for data input in compliance with the data minimisation principle.
- ○ Implement appropriate technical and organisational measures consistently and in a timely manner to protect the confidentiality, integrity, and availability of personal data.
- ○ Implement measures to restrict and record each access and use of personal data, as appropriate.
- ○ Personal data is securely disposed of in a way that renders data unrecoverable at the end of the retention period or other relevant event.

6. Access control

OBJECTIVE: Implement user access management based on least privilege and accountability and prevent unauthorised access to systems and applications.

- **Essential outcomes:**
  - Implement appropriate access control policy for physical and digital access defining access rules, rights, restrictions and controls.

- **Measures and controls**
- ○ Implement a formalised central process for requesting, approving and assigning access privileges.
- ○ Assign access in compliance with the principle of least privilege and based on the role in the organisation and business need for access.
- ○ No one person will have full unrestricted access. Administrator accounts will be monitored and subject to regular verification.
- ○ Adopt access policy which includes rules about user registration and deregistration, authorisation procedures, asset owner responsibilities, revoking access, regular review of IDs, monitoring, allocation of user privileges, regular review of access rights, management of secret authentication information such as passwords, and other matters.
- ○ A record of all users including their level of access must be maintained. HR notifies any pending terminations or known changes in business need for access.
- ○ Access privileges are regularly reviewed and access is removed promptly when the user is terminated or when no longer necessary in connection with their role or duties.
- ○ Identity verification protocols are implemented, as appropriate. Tech support team verifies identify before complying with request to reset password.
- ○ Access is password protected. Password standards meet industry best practices, including periodic renewal at least every six months.
- ○ The storage of passwords is encrypted.
- ○ Repeated unsuccessful attempts to gain access will result in a lockdown of the account.
- ○ Adequate measures are in place to limit the ability for personnel to store personal data on portable media or cloud.
- ○ Access to one system does not automatically grant access to another system.
- ○ Personal data is pseudonymised and anonymised, as appropriate.

7. Cryptography

OBJECTIVE: Ensure proper and effective use of cryptography to protect the confidentiality, authenticity and integrity of information.

- **Essential outcomes**
  - Implement policy to ensure appropriate use of cryptographic technologies and techniques and their proper management.

- **Measures and controls**
- ○ Design rules for the creation, distribution, changes, back up and storage of cryptographic key material throughout the lifecycle.
- ○ Minimise possibility to circumvent measures, as appropriate.
- ○ Provide training on the effective use of cryptography.

8. Physical and environmental security

OBJECTIVE: Prevent unauthorised physical access, loss, damage, theft or interference with the organisation's information assets and information processing facilities and any resulting interruption of operations.

- **Essential outcomes**
  - Define physical security perimeters to protect valuable information assets.
  - Manage risks of access points.
  - Implement physical security controls.
  - Protect against external and environmental threats.
  - Manage risks inside secure areas.

- **Measures and controls**
- Secure premises and facilities with appropriate lock systems.
- Secure offices, rooms and facilities by, for example, addressing who can see or hear into the office from outside, removing assets when not occupied and other measures.
- Restrict recording, unsupervised working, in and out monitoring and logging in relation to secure areas.
- Secure delivery and loading areas.
- Limit physical access to those with a business need, e.g. server rooms only accessible by designated IT personnel, access to equipment at the reception is restricted to designated reception personnel, etc.
- A manned reception is deployed at the entrance to business premises, where appropriate.
- Visitors are escorted, where appropriate.
- Security personnel patrols entrances and other areas to prevent unauthorised intrusion, theft, burglary and other criminal activities, where appropriate.
- CCTV is deployed where appropriate.
- Air temperature and humidity are set and monitored at appropriate levels for the computing equipment to operate.
- Deploy uninterruptible power supply modules and backup generators that provide back-up power in the event of an electrical failure for servers, where appropriate.

9. Equipment security

OBJECTIVE: Prevent loss, damage and theft or compromise of IT assets and interruption to the organisation's operations.

- **Essential outcomes**
  - Implement equipment sitting rules.
  - Implement supporting utilities.
  - Conduct regular equipment maintenance.
  - Manage assets taken or regularly used off-site.
  - Securely dispose of or re-use equipment.
  - Secure unattended equipment.

- **Measures and controls**
- Ensure that hardware and devices are only accessible by authorised personnel.
- Restrict viewing angle of screens, access to storage facilities, food and drink near devices, allow easy access to facilities such as printers, prohibit leaving printouts on printer and other measures, as appropriate.
- Ensure dual power supply, multiple routing of telecommunications equipment, load balancing and redundancy in switching equipment, bandwidth capacity monitoring, as appropriate.
- Ensure security of power and telecommunications cabling and comply with health and safety rules.
- Implement clear desk and screen policy.
- Ensure regular inspections and maintenance of devices.
- Implement secure configuration, patch management, real-time protection anti-virus, anti-malware and anti-spyware software, properly configured operation system and network firewalls, web filtering and other appropriate Internet access restrictions, encryption, as appropriate.
- Ensure timely decommissioning and secure wiping of old hardware is ensured.
- Enable remote wiping on corporate and BYOD devices.
- Securely dispose of tangible property containing personal data and electronic files.

10. Operations Security

OBJECTIVE: Ensure the correct and secure operation of information processing facilities.

- **Essential outcomes**
  - Implement standard operating procedures to ensure correct operation.
  - Implement capacity management to meet business objectives particularly in relation to data storage, processing power and communications bandwidth.
  - Ensure integrity of operation systems.
  - Implement a backup policy for software and system images to be taken and tested regularly.
  - Implement change management across the organisation.
  - Minimise negative effect on operational systems of audits, vulnerability scans and penetration tests.

- **Measures and controls**

- Synchronise clocks o all relevant information processing systems.
- Implement detection, prevention and recovery controls to protect against malware.
- Implement controls for the installation of software on operational systems and on local devices. Prevent installation of hacking tools.
- Keep records of regular tests of backups.
- Implement monitoring and event logging. Keep system logs, system administrator logs, system operator activity logs, access control logs, incident logs, etc.
- Protect log information in tamper-proof manner.
- Ensure access to information about vulnerabilities in a timely fashion.
- Implement process for audits, vulnerability scans and penetration tests including authorisation.
- Implement roll-back procedures.
- Implement secure vulnerability patches without delay.
- Implement application whitelisting (AWL).
- The company utilises a redundancy strategy to safeguard against failures of primary storage systems.
- Business continuity and disaster recovery plans are in place with assigned responsibilities in case of relevant events.
- Personal data and relevant applications are regularly backed up in accordance with industry best practices.
- Backups should be segregated from, and protected at the same level, as live environments.
- The success of backup cycles, integrity of backups and restoration procedures are tested regularly.

11. Communications Security

OBJECTIVE: Ensure the protection of information in networks, information processing facilities and information transferred within and outside the organisation.

- **Essential outcomes**
  - Manage and control networks to protect information assets.
  - Implement network services agreements defining security mechanisms, service levels and management requirements.
  - Implement segregation of information services, users and systems.
  - Implement transfer policies, procedures and controls to protect the transfer of information through all communications facilities.
  - Impose contractual obligation of confidentiality.
  - Provide appropriate training.

- **Measures and controls**

- Implement connection control, endpoint verification, firewalls, intrusion detection/prevention systems, access control lists, and physical, logical or virtual segregation.
- Segregate duties of network operations and system operations.
- Ensure networks are appropriately segmented and segregated.
- Implement agreements for transfers of data within and outside the organisation.
- Impose non-disclosure obligations in the form of non-disclosure agreements, customer terms, supplier or partner terms, employment terms and privacy policies and email footers.
- Implement measures to protect information from interception, copying, modification, mis-routing and destruction.
- Implement requirements around notifications, traceability, escrow, identification standards, chain of custody, cryptography, access control and others.

- Implement policies about electronic messaging.
- Implement multi-factor authentication in relation to VPN access.
- Hide admin console from public access, where appropriate.
- Deploy appropriately configured firewalls.
- Adopt Transport Layer Security for data transfers.
- Implement HTTP Strict Transport Security.
- Deploy intrusion prevention and detection software.
- Deploy real-time protection anti-virus, anti-malware and anti-spyware software with a threat database which is regularly updated.
- Deploy vulnerability scanning to monitor corporate networks for suspicious behaviour and vulnerabilities by lawful means.
- Carry out penetration testing and security assessments.
- Carry out server hardening.
- Access to corporate wi-fi is restricted and monitored. Corporate wi-fi is separate to public wi-fi.
- Implement policy for the sharing of personal data within and outside the organisation including rules about recipient due diligence, lawfulness of transfer, and compliance with international data transfer rules.

12. System acquisition, development & maintenance

OBJECTIVE: Ensure the security of information systems at development stage and throughout their lifecycle.

- **Essential outcomes**
  - Ensure that information security is an integral part of new system development or change to existing systems. Avoid retrofitting security capabilities.
  - Use secure development environments for system development and integration efforts.
  - Carry out appropriate due diligence and enter into appropriate agreements when outsourcing development.
  - Carry out acceptance testing for new information systems, upgrades and new versions, and the testing of security functionalities.
  - Ensure the maintenance of systems throughout their life cycle until decommissioning.
  - Ensure the timely decommissioning of outdated or unsupported systems.

- **Measures and controls**

- Adopt secure development policy explaining how security needs to be considered at all stages of the development lifecycle.
- Align software development methodology with appropriate security frameworks such as the OWASP secure web application framework. Adopt secure system engineering principles appropriate to the risks identified.
- Protect information from fraudulent activity, contract dispute and unauthorised disclosure and modification.
- Ensure confidentiality, integrity and availability of information in services provided over public networks.
- Protect service transactions to prevent incomplete transmission, mis-routing, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay.
- Implement system change control procedures aligned with operation change control and keep appropriate logs.
- Test operating system changes in a development or test environment where critical business applications can be checked for compatibility with the changed operating system.
- Review and test business critical applications after change to ensure there is no adverse impact on the organisational operations or security.
- Restrict changes to software packages.
- Maintain separate development, testing and operational environments.
- Protect test data and minimise use of live data for testing. Anonymise any live data used for testing.
- Implement electronic signatures, encryption secure protocols.
- Adopt “hardening” techniques appropriate for the coding language used.
- Implement inlife management.
- Adopt pair programming, peer reviews and independent quality assurance, code reviews and testing.
- Identify and address compatibility issues in a timely manner.
- Ensure the timely decommissioning of unsupported or incompatible software.
- Continuously test software and dependencies for vulnerabilities.

13. Supplier relationships

OBJECTIVE: Protect the organisation's assets accessed by suppliers and partners and maintain the level of information security mandated under relevant agreements.

- **Essential outcomes**
  - Implement information security policy for suppliers and partners.
  - Regularly monitor, review and audit supplier and partner service delivery.
  - Manage changes to supplier and partner services.

- **Measures and controls**
- Ensure proper supplier and partner segmentation, selection, management and exit.
- Carry out due diligence, enter into appropriate agreements and keep on-boarding records.
- Ensure legal review of supplier contracts.
- Enforce contracts without delay and do not waive your rights.
- Regularly monitor, review and audit their supplier service delivery and keep appropriate records.
- Carry out human relationship review and review of public security reviews and ratings.
- Carry out a data privacy impact assessment and security risk assessment to identify and address risks, where appropriate.
- Ensure the supplier and partner complies with its controller or processor obligations, as appropriate.
- Use a secure file transfer protocol and encrypt personal data, where appropriate.
- Require a certificate of destruction or deletion of personal data upon termination of the engagement or earlier relevant event.

14. Information security incident management

OBJECTIVE: Ensure a consistent and effective approach to management of the lifecycle of incidents, events and weaknesses.

- **Essential outcomes**
  - Establish responsibilities and procedures to ensure a quick, effective and orderly response to information security weaknesses, events and incidents.
  - Assign owners, actions and timescales in relation to the reporting, logging, handling and decision-making concerning information security weaknesses, events and incidents.
  - Adopt an incident response plan.
  - Reduce the likelihood or impact of any future incidents and adapt information security measures.

- **Measures and controls**
- Adopt incident response plan and related policies and procedures.
- Ensure effective collection of evidence.
- Ensure a good chain of custody.
- Train personnel on how to identify and report security incidents.
- Encourage the reporting of weaknesses, events and incidents.
- Ensure that personnel do not attempt to test weaknesses.
- Carry out root cause analysis and implement remediation plan in relation to each incident.
- Keep a log of each of weakness, event and incident, as appropriate.
- Comply with statutory notification obligations in relation to personal data breaches.

15. Information security aspects of business continuity management

OBJECTIVE: Ensure information security continuity and the availability of information processing facilities.

- **Essential outcomes**
  - Ensure the required level of continuity for information security during a disruptive situation.
  - Implement and review information security continuity policies and procedures.

- **Measures and controls**
- Define responsibilities, activities, owners, timescales, mitigating work to be undertaken in relation to information security continuity.

- Ensure that the controls implemented for information security continuity are tested, reviewed and evaluated periodically.
- Implement redundancy sufficiency with regular testing.

16. Compliance

OBJECTIVE: Avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and operate information security in accordance with the organisational policies and procedures.

- **Essential outcomes**
  - Understand and comply with applicable laws and contractual obligations.
  - Implement security policies, procedures, controls and measures on a proactive as well as reactive basis, as appropriate.

- **Measures and controls**
- Engage legal experts for legal advice, where appropriate.
- Ensure independent review of security risks and controls.
- Implement security controls and measures on a proactive and reactive basis.
- Design customer terms in a way that reflects your risk profile.

Prepared by:

Alex Dittel – Senior Associate at Kemp Little LLP, alex.dittel@kemplittle.com
James Bore - Cyber Security Consultant at Bores Consultancy Ltd, james@bores.com

Other resources:

- **Data protection guide**
  https://www.kemplittle.com/publications/kldemystify-data-protection-complete-guide/

- **Cybersecurity toolkit**
  https://www.kemplittle.com/publications/cybersecurity-toolkit/