Internal Audit Checklist

AUDIT	
AUDIT SCOPE	
AUDITOR(S)	
DATE Of AUDIT	

4 Context of the Organisation

4.1 Understanding the organisation and its context

Recommended Questions	Audit Findings	Evidence Reviewed
1. What are the internal and external issues that are relevant to the ISMS?		
2. How do they affect its ability to achieve its intended outcome?		

4.2 Understanding the needs and expectations of interested parties

Recommended Questions	Audit Findings	Evidence Reviewed
1. Who are the interested parties?		
2. What are their requirements?		
3. How have their requirements been established?		

4.3 Determining the scope of the ISMS

Recommended Questions	Audit Findings	Evidence Reviewed
1. What is the ISMS scope?		
2. How is it defined?		
3. Is it reasonable?		
4. Does it consider relevant issues and requirements?		
5. Does it consider how the organization interacts with other organizations?		
6. Is the scope documented?		

5 Leadership

5.1 Leadership and Commitment

Recommended Questions	Audit Findings	Evidence Reviewed
1. Who is defined as top management within the scope of the ISMS?		
2. How does top management demonstrate leadership and commitment?		
3. Are information security policies and objectives 4. established?		
5. Are enough resources allocated to the ISMS?		
6. How does top management communicate to everyone involved in the ISMS?		

5.2 Policy

Recommended Questions	Audit Findings	Evidence Reviewed
1. Can I review the information security policy?		
2. Is it appropriate and cover the required areas?		
3. Does it include the required commitments?		
4. How has it been communicated and distributed and to whom?		

5.3 Organizational roles, responsibilities and authorities

Recommended Questions	Audit Findings	Evidence Reviewed
1. What are the roles within the ISMS?		
2. Does everyone understand what their responsibilities and authorities are?		
3. Who has the responsibility and authority for conformance and reporting?		

6 Planning

6.1 Actions to address risks and opportunities

Recommended Questions	Audit Findings	Evidence Reviewed
1. Is there a documented risk assessment process?		
2. Does it address risk acceptance criteria and when assessments should be done7		
3. What is the most recent risk assessment?		
4. Does it identify a reasonable set of risks and specify owners?		
5. Are the likelihood and impact of risks assessed appropriately and risk levels determined?		
6. How are the risks then evaluated and prioritized?		
7. Is there a documented risk treatment process?		
8. Review the most recent risk treatment plan.		
9. Are reasonable risk treatment options selected?		
10. Are the controls chosen to treat the risks stated dearly?		
11. Has a Statement of Applicability been produced and are inclusions and exclusions reasonable?		
12. Has the risk treatment plan been signed off by the 13. risk owners?		

6.2 Information security objectives and planning to achieve them

Recommended Questions	Audit Findings	Evidence Reviewed
1. Are there documented 2. information security objectives?		
3. Do the objectives comply with section 6.2 (a) to (e)?		
4. Is there a plan to achieve the objectives?		
5. Are all the elements in 6.2 (f) to (j) included?		

7 Support

7.1 Resources

Recommended Questions	Audit Findings	Evidence Reviewed
1. How are the resources needed for the ISMS determined?		
2. Are the required resources provided?		

7.2 Competence

Recommended Questions	Audit Findings	Evidence Reviewed
1. Havethe necessary competences been determined?		
2. How has the competence of the people involved in the ISMS been established?		
3. What actions have been identified to acquire the necessary competence?		
4. Have they been completed and is there evidence of this?		

7.3 Awareness

Recommended Questions	Audit Findings	Evidence Reviewed
1. What approach has been taken to providing awareness of the information security policy, contribution to the ISMS and implications of not conforming?		

2. Has everyone been covered?		

7.4 Communication

Recommended Questions	Audit Findings	Evidence Reviewed
1. How has the need for communication been established?		
2. Is the approach to communication documented?		
3. Does the approach cover all areas in 7.4 (a) to e)?		

7.5 Documented information

Recommended Questions	Audit Findings	Evidence Reviewed
1. Is all the documented information required by the 2. standard in place?		
3. Is the level of other documentation reasonable for the size of ISMS?		
4. Are appropriate documentation standards - for example, identification, format - in place?		
5. Are the standards applied in a uniform way?		
6. Are appropriate controls in place to meet 7.5.3 (a) to (f)?		
7. How are documents of external origin handled?		

8 Operation

8.1 Operational planning and control

Recommended Questions	Audit Findings	Evidence Reviewed
1. What plans are available to review?		
2. Do they cover requirements, objectives and risk treatments?		
3. What planned changes have taken place recently and how were they controlled?		
4. What processes are outsourced?		
5. How are they controlled?		

8.2 Information security risk assessment

Recommended Questions	Audit Findings	Evidence Reviewed
1. What are the planned intervals for risk assessments?		
2. What significant changes have happened that have prompted a risk assessment to be carried out?		

8.3 Information security risk treatment

Recommended Questions	Audit Findings	Evidence Reviewed
1. What is the status of the risk treatment plan(s)?		
2. How is it updated?		
3. How is the success of the treatment judged?		

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

Recommended Questions	Audit Findings	Evidence Reviewed
1. How is it determined what should be monitored and measured?		
2. Review evidence of monitoring and measurement.		
3. What procedures are in place to cover monitoring and measurement in different areas?		
4. How are results reported?		

9.2 Internal audit

Recommended Questions	Audit Findings	Evidence Reviewed
1. How often are internal audits carried out?		
2. Who carries them out?		
3. Are the auditor's objective and impartial?		
4. Review the most recent internal audit report.		
5. Have any nonconformities resulting from previous audits been addressed?		
6. Does the audit programme cover the complete scope of the ISMS?		

9.3 Management review

Recommended Questions	Audit Findings	Evidence Reviewed
1. How often are management reviews carried out?		
2. Who attends them?		
3. Are they minuted?		
4. Review the results of the most recent one.		
5. Are all areas in 9 .3 a) to f) covered at management reviews?		
6. Does the management review represent a reasonable assessment of the health of the ISMS?		

10 Improvement

10.1 Nonconformity and corrective action

Recommended Questions	Audit Findings	Evidence Reviewed
1. How are nonconformities identified?		
2. How are they recorded?		
3. Review the records of a recent nonconformity.		
4. Was appropriate action taken to correct it and address the underlying causes?		
5. Was the effectiveness of the corrective act ion reviewed?		

10.2 Continual improvement

Recommended Questions	Audit Findings	Evidence Reviewed
1. How are improvements identified?		
2. Are they recorded?		
3. What evidence of continual improvement can be demonstrated?		

Annex A Reference Controls (NB: not all may be applicable)

A5 Information security policies

Recommended Questions	Audit Findings	Evidence Reviewed
1. Review the set of policies.		
2. Are they all approved?		
3. Who have they been communicated to?		
4. When was the last time they were reviewed?		

A6 Organisation of information security

Recommended Questions	Audit Findings	Evidence Reviewed
1. Where is segregation of duties used within the organization?		
2. Which relevant authorities and special interest groups is contact maintained with and how?		
3. How was information security addressed in the most recent project?		
4. Is there a mobile device policy?		
5. What security measures are used to manage mobile device risks?		
6. Is there a teleworking policy?		
7. Review the security measures in place at a specific teleworking site.		

A7 Human resource security

Recommended Questions	Audit Findings	Evidence Reviewed
1. What background verification checks are carried out on employment candidates?		
2. How is information security covered in employment contracts?		
3. How are employees and contractors made aware of, and trained in, information security issues?		
4. Is there a formal disciplinary process?		
5. What happens when an employee leaves, with respect to information security?		

A8 Asset management

Recommended Questions	Audit Findings	Evidence Reviewed
1. Is there an asset inventory?		
2. Are all assets in the inventory owned?		
3. Are rules fort the acceptable use of assets identified, documented and implemented?		
4. What happens to assets when an employee leaves?		
5. Is there an information classification scheme in place?		
6. How is information labelled with its classification?		
7. What procedures are in place for handling high value assets?		
8. How is removable media managed, including disposal and transport?		

A9 Access control

Recommended Questions	Audit Findings	Evidence Reviewed
1. Is there an access control policy?		
2. How is it decided which networks and network services a user is authorized to?		
3. Is there a formal registration and de-registration process?		
4. Is there a formal user access provisioning process?		
5. How are privileged access rights controlled?		
6. Is there a formal management process to allocate secret authentication information?		
7. How are access rights reviewed and how often?		
8. What happens to access rights when someone moves or leaves?		
9. How is the access control policy implemented within applications e.g. logons, passwords?		
10. How is the use of utility programs controlled?		
11. Is access to program source code restricted?		

A10 Cryptography

Recommended Questions	Audit Findings	Evidence Reviewed
1. Is there a policy on the use of cryptographic controls?		
2. How has it been implemented?		
3. Is there a policy covering cryptographic keys?		
4. How has it been implemented?		

A11 Physical and environmental security

Recommended Questions	Audit Findings	Evidence Reviewed
1. Have the physical security perimeter and secure areas been defined?		
2. What physical entry controls are in place		
3. What physical protections are in place to guard against natural disasters, malicious attack or accidents?		
4. Are there procedures for working in secure areas?		
5. What controls are in place over delivery and loading areas?		
6. How is it decided where to site equipment?		
7. What protection is in place from failures of supporting utilities?		
8. Is important cabling protected?		
9. Review equipment maintenance logs.		
10. What is the procedure for taking assets offsite and how are they protected whilst offsite?		
11. How is storage media disposed of securely?		
12. Is there any unattended equipment that requires protection and if so, how is that provided?		

13. Are desks and screens clear of sensitive information and storage media?		

A12 Operations security

Recommended Questions	Audit Findings	Evidence Reviewed
1. To what extent are operating procedures documented?		
2. How are changes controlled?		
3. How is capacity managed?		
4. Are development, testing and operational environments separated?		
5. What controls are in place to handle malware?		
6. How aware are users of the threat from malware?		
7. What is the backup policy and process of the organization?		
8. Are event logs collected and protected from tampering?		
9. Are system administrator and operator activities logged and reviewed?		
10. How are the clocks of the various infrastructure components synchronized?		
11. How is software installation on operational systems controlled, both at a system and user level?		
12. How are technical vulnerabilities identified and addressed?		

13. How are audits carried out without disrupting business processes?		

A13 Communications security

Recommended Questions	Audit Findings	Evidence Reviewed
1. How is network security managed and controlled?		
2. Are network services agreements in place for all relevant services?		
3. Do they cover security mechanisms, service levels and management requirements?		
4. Is network segregation used and if so how?		
5. What information transfers take place?		
6. Are there policies, procedures and controls in place to protect them?		
7. Are controls documented in formal agreements?		
8. How is electronic messaging protected?		
9. Are there non-disclosureagreements in place with key parties?		

A14 System acquisition, development and maintenance

Recommended Questions	Audit Findings	Evidence Reviewed
1. Are information security requirements included in specifications for new or changed systems?		
2. How is information passing over public networks e.g. the Internet, protected?		
3. For each type of application service, how are transactions protected from known threats?		
4. How is software developed securely within the organization?		
5. Is change control in place in the development lifecycle?		
6. What process is performed when operating platforms are changed?		
7. How much change is made to commercial off -the-shelf software?		
8. What principles are used when engineering secure systems?		
9. How are development environments protected?		
10. How do you monitor outsourced software development?		
11. To what extent is system security tested during development?		

12. Review records of acceptance testing for most recent system implementation		

A15 Supplier relationships

Recommended Questions	Audit Findings	Evidence Reviewed
1. How are the organisation's security requirements communicated and agreed with suppliers?		
2. To what extent are the requirements documented in supplier agreements?		
3. Do agreements with suppliers require them to address security risks?		
4. How is supplier service delivery monitored, reviewed and audited?		
5. How are changes made by suppliers managed and risk-assessed?		

A16 Information security incident management

Recommended Questions	Audit Findings	Evidence Reviewed
1. Is there an information security incident procedure?		
2. Are incident management responsibilities understood?		
3. How are information security events and weaknesses reported?		
4. How is the decision about whether to classify an event as an incident made?		
5. Review how some of the most recent incidents were responded to.		
6. How is knowledge gained from incidents re-used?		
7. Are procedures in place to ensure that potential evidence is protected?		

A17 Information security aspects of business continuity management

Recommended Questions	Audit Findings	Evidence Reviewed
1. Are information security requirements in the event of a disaster understood?		
2. Do business continuity procedures provide for the required level of information security?		
3. Are the procedures tested regularly?		
4. Are availability requirements identified and is enough redundancy in place to meet them?		

A18 Compliance

Recommended Questions	Audit Findings	Evidence Reviewed
1. Is it clear which laws and regulations apply to the organization and its activities?		
2. Are contractual obligations understood?		
3. Is an approach to meet these requirements in place?		
4. Are procedures implemented to ensure compliance with intellectual property rights?		
5. Are records protected in line with the understood requirements?		
6. Is privacy and protection of personally identifiable information addressed adequately?		
7. Is the organization's use of cryptographic controls legal and compliant with relevant agreements?		
8. How often are independent reviews of information security carried out?		
9. How often do managers check their areas comply with information security policies and standards?		
10. Review the most recent report on compliance of information systems with agreed information security policies.		