Section 1 Worth 40 marks. Answer all 10 questions.

Each question is worth 2 marks

1.01 What does the term “SoA” stand for in ISO 27001?
   a) Security of Assets
   b) Statement of Assessments
   c) Statement of Applicability
   d) Security of Assurance
   e) None of the above

1.02 What security requirements should be included in an outsourcing contract?
   a) Intellectual property rights
   b) Confidentiality, integrity, and availability
   c) Access control agreements
   d) Legal requirements
   e) All of the above

1.03 What part of ISO 27001 address the protection for website (home page) security?
   a) Communications and operations management
   b) Access control
   c) System development and maintenance
   d) Conformance
   e) None of the above

1.04 What type of risk assessment methods should be used by an organization in implementing an ISMS?
   a) Simple
   b) Detailed
   c) Systematic
   d) Combined
   e) None of the above

1.05 Which should be included in security training for employees?
   a) Information security policies
   b) Security incidents
   c) Information classification and labelling
   d) Security vulnerability, threats, risks
   e) All of the above

1.06 “Ensuring that information is accessible only to those authorised to have access” is:
   a) Privileged information
   b) Employees right of access
   c) Confidentiality
   d) Information conditions
   e) None of the above

1.07 Certification of an organization’s ISMS is to standard:
   a) ISO/IEC 17799:2005
   b) ISO/IEC 27001:2005
   c) ISO 19011:2011
   d) All of the above
   e) None of the above
1.08 Risk analysis is:
   a) Coordinated activities to direct and control an organization with regard to risk
   b) Treatment process of selection and implementation of measures to modify risk
   c) Decision to accept a risk
   d) Systematic use of information to identify sources and to estimate risk
   e) None of the above

1.09 A documented procedure according to ISO 27001 is required for:
   a) Management review
   b) Management responsibility
   c) Improvement of ISMS
   d) Corrective action
   e) None of the above

1.10 "Back-up copies of essential business information and software shall be taken and tested regularly" is called
   __________________________and covered by Clause No........

Section 2 is worth 60 marks.

The following two incidents were identified during a third party audit of an organization’s ISMS. They
contain situations for which a non-conformity report (NCR) may be required. Examine each incident
carefully then take one of the following actions:
   a) If you think there is sufficient objective evidence of non-conformity then you should complete a
      non-conformity report and categorize it as a Major or Minor.
   b) If you do not think there is sufficient objective evidence to raise a non-conformity report then
      you should state your reasons in the space below the report. You must also state what the
      auditor should do next.

4.01 Incident Number 1
During a third party audit of a multi-site banking organization, it was established during a branch office
audit, that the Policy and Statement of Applicability Policy are approved and signed by top managers of
the corporate head office who provide the security resources. The security officer working at the branch
office during the third party certification audit of this branch was employed by another branch office.

4.02 Incident Number 2
During a third party audit of a Financial Services Organization, the auditor identified evidence of an
employee who had accidentally breached the organization’s security policy regarding information
provided to clients. This was reported to the security manager and a security incident was recorded.
The security manager had issued an email to all employees re-stating the security policy and that
procedures would be reviewed and re-issued. No further occurrence had been recorded since issue of
the email but the procedure had not been reviewed or re-issued.