CENTRE ™ (Common Enterprise Resource)

Information Security Management System designed for ISO 27001:2005 (ISMS)

ISO/IEC 27001:2005 is the international standard for entities to manage their Information Security. It sets out how a company should address the requirements of **confidentiality**, **integrity** and **availability** of its information assets and incorporate this into an Information Management Security System (ISMS).

ISO/IEC 27001:2005 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization's overall business risks.

Certification to ISO/IEC 27001 is a powerful demonstration of an organization's commitment in managing information security. Attaining the standard makes a public statement of capability without revealing security processes or opening systems to second party audits. Many companies require certification to ISO/IEC 27001 as a prerequisite for doing business**.**

The standard ensures that controls are in place to reduce the risk of security threats and to avoid system weaknesses being exploited. It will also help an organization to develop a business continuity plan that will minimize the impact of security breaches.

Unprotected systems are vulnerable to computer-assisted fraud**,** sabotage and viruses**.** Breaches in information security can allow vital information to be accessed**,** stolen**,** corrupted or lost**.** An effective 'ISMS' will identify and clarify existing information security management processes and incorporate them into the procedures

CENTRE was developed to facilitate today's Best Practices Certifications. By using CENTRE, businesses can increase efficiencies across key business processes and satisfy many of the requirements stipulated by international standards boards. Some of the benefits that may be derived by using CENTRE are:

- Cost Reduction
- Compliance (Sarbanes Oxley, ISO/IEC, etc.)
- Reducing IT Complexity
- Process Improvement
- Business Process Alignment
- Operational Efficiency
- Integration & Standards

As a result, an organization using CENTRE will be recognized as delivering successful, secure service to its clients and constituents with dependably high-quality and consistent methods and practices.

Integration Technologies Group, Inc.

CENTRE's ISO/IEC 27001 _includes_ the CENTRE ISO 9001:2008 'Quality Management System' and CENTRE ISO 20000:2011 'Information Technology Service Management' elements.

These elements are described in greater detail on the 'CENTRE ISO 9001 Compliance Package' and 'CENTRE ISO 20000 ITSM Compliance Package' White Papers.

The following CENTRE elements are listed with their corresponding ISO 27001 clauses and Annex 'A' Sections:

- CENTRE – Document Control System (DCS)
  Section 4.3.2 - Control of Documents
    Annex-A.15 - Compliance
      Subsection   A.15.1.3 - Protection of organizational records

- CENTRE – Records Control System (RCS)
  Section 4.3.3 - Control of Records
    Annex-A.15 - Compliance
      Subsection   A.15.1.3 - Protection of organizational records

- CENTRE – Human Resources
  Section 5.2.2 - Resource Management/Training, Awareness, and Competence
    Annex-A.8 - Human Resources Security
      Subsections   A.8.1 - Prior to Employment
                    A.8.2 - During Employment
                    A.8.3 - Termination or Change of Employment
- CENTRE – Meeting Management
  Section 4.2.3 - Monitor and Review the ISMS
  Section 7 - Management review of the ISMS
    Annex-A.5 - Security Policy
      Subsection   A.5.1.2 - Review of the Information Security Policy

- CENTRE – Customer Satisfaction Surveys
  Section 7.2 - Review input
    b) Feedback from interested parties
    h) Any changes that could affect the ISMS
    i) Recommendations for improvement

- CENTRE – Supply Chain Management
  Annex-A.6.2 - External Parties
    Subsections   A.6.2.1 - Identification of risks to external parties
                  A.6.2.2 - Addressing security when dealing with customers
                  A.6.2.3 - Addressing security in third party agreements
  Annex-A.7 - Asset Management
  Annex-A.7.1 - Responsibility for assets
    Subsections   A.7.1.1 - Inventory of Assets
                  A.7.1.2 - Ownership of Assets
                  A.7.1.3 - Acceptable use of Assets
  Annex-A.10.2 - Third party service delivery management

Integration Technologies Group, Inc.

Subsections   A.10.2.1 - Service delivery
    A.10.2.2 - Monitoring and review of third party Services
    A.10.2.3 - Managing changes to third party services
    Annex- A.10.8 - Exchange of Information

- CENTRE – Ad-Hoc Report Writer
  - Section 4.2.3 - Monitor and Review the ISMS
    - Annex-A.10.10 - Monitoring
      - Subsection   A.10.10.2 - Monitoring system use

- CENTRE – Contract Management
  - Section 4.2.1 - Establish the ISMS
    - d) Identify the risks
      - 1) Identify the assets within the scope of the ISMS, and the owners of these assets.
      - 2) Identify the threats to those assets
      - 3) Identify the vulnerabilities that might be exploited by the threats
      - 4) Identify the impacts that losses of confidentiality, integrity and availability may have on the assets
    - e) Analyze and evaluate the risks
    - Annex-A.6.1 - Internal organization
      - Subsection   A.6.1.5 - Confidentiality agreement
    - Annex-A.10.2 - Third party service delivery management
      - Subsections   A.10.2.1 - Service delivery
      - A.10.2.2 - Monitoring and review of third party Services
      - A.10.2.3 - Managing changes to third party services
    - Annex-A.10.8 - Exchange of Information
      - Subsections   A.10.8.1 - Information exchange policies and procedures
      - A.10.8.2 - Exchange agreements

- CENTRE – Configuration Item Management
  - Annex-A.7 - Asset Management
  - Annex-A.7.1 - Responsibility for assets
    - Subsections   A.7.1.1 - Inventory of Assets
    - A.7.1.2 - Ownership of Assets
    - A.7.1.3 - Acceptable use of Assets

- CENTRE – Incident Management/Problem Management
  - Section 4.2.2 - Implement and Operate the ISMS
    - h) Record actions and events that could have an impact on the effectiveness or performance of the ISMS, Monitor and Review the ISMS
  - Section 4.2.3 - Monitor and review the ISMS, Execute monitoring and reviewing procedures and other controls to:
    - 1) Promptly detect errors in the results of processing
    - 2) Promptly identify attempted and successful security breaches and incidents
    - 3) Enable management to determine whether the security activities delegated to people or implemented by information technology are performing as expected
    - 4) Help detect security events and thereby prevent security incidents by the use of indicators
    - 5) Determine whether the actions taken to resolve a breach of security were effective.
  - Section 4.2.1 - Establish the ISMS

Integration Technologies Group, Inc.

h) Record actions and events that could have an impact on the effectiveness or performance of the ISMS

    Section 4.3.3 - Control of Records

    Annex-A.13 - Information security incident management

    Annex-A.13.1 - Reporting information security events and weaknesses

        Subsections   A.13.1.1 - Reporting information security events

                       A.13.1.2 - Reporting security weaknesses

    Annex-A.13.2 - Management of information security incidents and improvements

        Subsections   A.13.2.1 - Responsibilities and procedures

                       A.13.2.2 - Learning from information security incidents

                       A.13.2.3 - Collection of evidence

- CENTRE – Change Management

    Annex-A.10 - Communications and operations management

        Subsection   A.10.1.2 - Change management

    Annex-A.12.5 - Security in development and support processes

        Subsection   A.12.5.1 - Change control procedures

- CENTRE – Release Management

    Annex-A.10 - Communications and operations management

        Subsection   A.10.1.2 - Change management

    Annex-A.12.5 - Security in development and support processes

        Subsections   A.12.5.1 - Change control procedures

                       A.12.5.2 - Technical review of applications after operating system changes

                       A.12.5.3 - Restrictions on changes to software packages

                       A.12.5.4 - Information leakage

                       A.12.5.5 - Outsourced software development

- CENTRE – Project Management

    Section 4.2.1 - Establish the ISMS

        e) Analyze and evaluate the risks (sections 1 through 4)

        f) Identify and evaluate options for the treatment of risks (sections 1 through 4)

        g) Select control objectives and controls for the treatment of risks

        Annex-A.14.1- Information security aspects of business continuity management

            Subsection   A.14.1.2 - Business continuity and risk assessment

- CENTRE – Financial Management

    Section 5.1 - Management commitment

    Section 5.2.1 - Provision of resources, The organization shall determine and provide the resources needed to:

        a) Establish, implement, operate, monitor, review, maintain and improve an ISMS

        c) Identify and address legal and regulatory requirements and contractual security obligations

    Section 7.3 - Review output, the output from the management review shall include any decisions and actions related to the following;

        d) Resource needs

        Annex-A.10.3 - System planning and acceptance

            Subsection   A.10.3.1 - Capacity management

- CENTRE – Measurement and Analysis Reporting

Section 4.2.3 - Monitor and review the ISMS
Section 8.1 - Continual improvement
   3) Enable management to determine whether the security activities delegated to people or implemented by information technology are performing as expected