Janco Associates, Inc.

Disaster Recovery / Business Continuity Audit Program

• • •

ISO 28000 – Supply Chain
ISO 27000 Series
ISO 22301:2023
CCPA - GDPR - HIPAA
Sarbanes-Oxley
PCI-DSS
BYOD – Mobile Devices
IoT
Artificial Intelligence

• • •

2024 Edition

Auditor Consideration

- **Security -** Application systems are connected to the Internet, so they are prone to attacks from cyber criminals and hacktivists. Among other information security audit procedures, IT auditors should perform a vulnerability assessment of all Internet-connected devices and consider conducting penetration tests on those systems periodically. The results of these procedures should be used to strengthen the security of systems, where necessary. Auditors should carefully consider where third parties are involved in supporting systems and assess whether third parties have adequate security controls in place to protect data residing in systems. Furthermore, they should assess the adequacy of the encryption of all systems used for communication.

- **Resilience -** Application systems may support a business process that is critical or time-bound, such as the delivery of perishable goods. IT auditors should assess whether controls are in place to recover systems in the event of failure. Auditors should determine whether management understands the potential business impact of a system outage and whether appropriate and adequate policies, procedures, and processes are in place to recover affected business processes timely in the event of an outage or disaster.

- **Health and Safety -** Many of today's systems c t area internal auditors should assess is whether all systems have undergone sufficient testing usir n. Furthermore, controls should be in place to ensure adequate testing is performed before upgrade d safety are a significant risk.

- **Monitoring -** Like any other business process, nctioning as intended. Internal auditors should assess whether adequate monitoring controls are in p ively over time. Furthermore, auditors should assess whether exceptions and failures that occur are logged appropriately and whether resolutions to incidents are recorded timely. Auditors also should assess whether management has a process that takes recurring incidents into account and analyzes their root causes.

- **Scoping of business unit operational systems -** Today many vendor-provided systems can be simple to implement, some systems may be deployed by business units without the IT department's involvement. For example, fire detection systems in enterprise facilities may have IoT capability that the IT department does not know about and risk management professionals and internal auditors may not notice. Auditors should be vigilant to see where and when systems are deployed by different departments in the organization and prioritize systems audits according to their criticality and sensitivity.

ISO 22301

- **Objectives and monitoring performance** – While continuity objectives were required in BS 25999, the requirement for them to be measurable was not specifically defined. ISO 22301 changes this by emphasizing measurable objectives as well as an emphasis on monitoring performance.
- **Terms and Definitions** – The terms and definition se[illegible]des references to terms that have been common in business continuity such as RPO (Recovery Point [illegible]
- **Legal and Regulatory Requirements** – Similar to ISO[illegible]ganization to establish, implement, and maintain a procedure to identify, have access to, and assess t[illegible]ation as they relate to the continuity of its operations, products, services, and the interests of i[illegible]
- **Communication** – There is an expanded communica[illegible]communication plans for internal and external interested parties.
- **Business Continuity Strategy** - BS 25999 did an excellent laying out a framework for Business Impact Analysis and Risk Assessment. ISO 22301 goes into much more detail on business continuity strategy.
- **Alignment to other Management System Standards** – BS 25999 was not a fully integrated management system standard; although many companies implemented BS 25999 as if it was a full management system ISO 22301. ISO 22301 follows the new requirements and alignment for all management system standards and is the 1st new standard to adopt these practices.

ISO 28000

Specifies the requirements for a security management system, including those aspects critical to the security assurance of the supply chain. Security management is linked to many other aspects of business management. Aspects include all activities controlled or influenced by organizations that impact supply chain security. These other aspects should be considered directly, where and when they have an impact on security management, including transporting goods along the supply chain.

ISO 28000 was developed by t ogy". It is based on the ISO format adopted by ISO 14001:2004 because of its risk-based approach to manag f:

- ISO 28000:2007 – The , a specification for an SMS against which organizations can certify compliance.
- ISO 28001:2007 – Prov nal supply chains.
- Assists in meeting the ed in the World Customs Organization Framework of Standards and conforming to national supply cha
- ISO 28002:2010 PAS - Development of resilience in the supply chain - Requirements with guidance for use.
- ISO 28003:2007 - Requirements for bodies providing audit and certification of supply chain security management systems
- ISO 28004:2007 - provides generic advice on the application of ISO 28000:2007.
- ISO/AWI 28005 – (Under development) Electronic port clearance (EPC) -- Part 1: Message structures.
- ISO/AWI 28005 – Electronic port clearance (EPC) -- Part 2: Core data elements

ISO 27000 (formerly ISO 17799)

The ISO/IEC 27000 series comprises information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The series contains best practice recommendations on information security management for use by IT management for initiating, implementing, or maintaining Information Security Management Systems (ISMS) and a growing family of related ISO/IEC ISMS standards.

ISO 27001 is part of the ISO/IEC 27000 series and is an Information Security Management System (ISMS) standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Its full name is *ISO/IEC 27001:2005 - Information Technology -- Security Techniques -- Information Security Management Systems -- Requirements* but it is commonly known as "ISO 27001." This standard is used in conjunction with ISO27002 (ISO27002), the Code of Practice for Information Security Management, which lists security control objectives and recommends a range of specific security controls. Organizations that implement ISMS per the best practice advice in ISO27002 are likely simultaneously to meet the requirements of ISO/IEC 27001.

ISO 27002 provides best practice recommendation esponsible for initiating, implementing, or maintaining Information Security Management Systems (ISMS). The standa

- Risk Assessment
- Security policy - management direction
- Organization of information security - g
- Asset management - inventory and clas
- Human resources security - security aspects for employees joining, moving, and leaving an organization
- Physical and environmental security - protection of the computer facilities
- Communications and operations management - management of technical security controls in systems and networks
- Access control - restriction of access rights to networks, systems, applications, functions, and data
- Information systems acquisition, development, and maintenance - building security into applications
- Information security incident management - anticipating and responding appropriately to information security breaches
- Business continuity management - protecting, maintaining, and recovering business-critical processes and systems
- Compliance - ensuring conformance with information security policies, standards, laws, and regulations

Certification to the 27000 standards is an optional step that can be taken at an enterprise's option. Since we continually update our products and the standards organizations continue to modify and enhance the standards we have chosen not to obtain formal certification at this time. To the best of our knowledge, this audit program is compliant with the ISO 27000 series of standards.

Audit Scope

There are dozens of security and compliance mandates that enterprises of all sizes need to address. The scope and content of each audit requirement need to be well understood. In addition, it is not productive to create unique audit programs for each mandate. Rather it is more cost-effective to include each mandate in an overall Compliance Management Audit Program. Below listed are the scope of the Annual, Semi-Annual, and Quarterly audit programs.

Annual Audit Scope

- **Active Directory Terms vs. Systems Terms** - Conduct an annual audit/comparison of terminations in Active Directory vs. terminations in all systems
- **Verify Accounts with Administrative Privileges Audits** - Core Systems Run audits listing all users who have administrative privileges to core systems. Administrative privileges will be validated via an enterprise's role-based access matrix.

Semi-Annual Audit Scope

- **Disaster Recovery Plan Test / Audit - Local the enterprise's Data Center** - Conduct a tabletop test of the local enterprise's disaster recovery/business continuity plan and update as required for change management.

Quarterly Audit Scope

- **Change of Status Workforce Audits**
- **Cybersecurity Tactical Simulations**
- **Day of Week / Time of Day Audit**
- **Departmental Downtime Procedures - Mock Test Audits**
- **Disabled AD Accounts Deletion Audits**
- **Random Audits**
- **Intrusion Vulnerability Audit**
- **PCI Data in Transit Audit**
- **Random Facility Walk-Through Audits**
- **Terminated Workforce Audits**
- **Verify Accounts with Administrative Privileges Audits**
- **Virus Detection Alerts**

Disaster Recovery / Business Continuity Audit Program

Site Audit and Risk Summary for Disaster Recovery and Business Continuity

It is unlikely that any activity or system can operate in complete isolation; rather they need to interact with other locations, data, and systems to be fully effective. It is often at the point of interaction between them where controls are critical. Auditors should be satisfied that the data moving between locations and systems is consistent, complete, and accurate so that the subsequent processes are undertaken on a reliable basis.

The following table aims to summarize the audit results of the site audits for Disaster Recovery/Business Continuity, and the potential interfaces with other systems which may require audit attention. The sites defined in this table are generic and need to be modified by the user of the Audit Program to be specific to the enterprise. The Risk Ranking is the number of No's that are recorded on the audit for each of the functions.

Site	Audited by	Date Completed	Risk Score and Level		Site	Audited by	Date Completed	Risk Score and Level
Corporate Office								
Warehouse								
Customer Service Center								
Administrative Office								
Outsourced Processing Center								
Corporate Data Center								
Branch Office								
BYOD – Mobile Devices								
Distribution Port								
Help / Service Desk Center								

Disaster Recovery / Business Continuity Audit Program

Company:	**Division:**	**Country:**	**Site:**
Audit Ref.:	**Date:**	**Completed by:**	**Reviewed by:**

Control Objective(s):

(a) To ensure that adequate and effective contingency plans have been established to support the prompt recovery of crucial enterprise functions and IT facilities in the event of major failure or disaster;
(b) To ensure that all mandated disaster recovery [illegible] ance policies and procedures in place;
(c) To ensure the survival of the business and to n[illegible]
(d) To ensure that all the potential risks to the ent[illegible] r the contingency plans;
(e) To ensure the optimum contingency arrangem[illegible]
(f) To ensure that an authorized and documented[illegible] o-date, and securely stored;
(g) To ensure that the recovery plan is periodically[illegible]
(h) To ensure that all internal and external parties[illegible] nmitments;
(i) To ensure that appropriate liaison is maintaine[illegible]);
(j) To ensure that both the damaged and recovery sites are secure and that systems are securely operated in support of the enterprise;
(k) To ensure that systems and procedures are adequately and accurately documented to aid the recovery process;
(l) To ensure that public and media relations would be effectively addressed during an emergency to minimize adverse publicity and business implications.

DRP and Business Continuity Audit Program							
Ref		Current Control/Measure/ Policy / Document / Comment	WP Ref.	Meet Requirement	Compliance Testing	Substantive Testing	Weakness to Report
General Considerations							
1.01	In the event of a disaster or significant disruption, does your organization have documented plans for business continuity and IT disaster recovery[2]?			**Yes / No**			
1.02	Has the enterprise considered the potential for all disaster types, the relevant risks, and the implications for the business operations?						
1.03	What type of failure scenarios or outages does the enterprise plan for? (a) Fire (b) Flood (c) Earthquake (d) Terrorist Attack (e) Hurricane (f) Tornado (g) Other: a. _____ b. _____ c. _____ d. _____			**Yes / No** **Yes / No** **Yes / No** **Yes / No** **Yes / No / NA** **Yes / No / NA** **Yes / No / NA** **Yes / No / NA** **Yes / No / NA** **Yes / No / NA**		

[2] A template of a Disaster Recovery / Business Continuity Plan can be found at https://e-janco.com/drp.htm

What's New

2024

- Update to cover include AI implications
- Corrected minor errata

2023

- Added section on audit scope
- Update to cover 28000 – Supply Chain Security Management System (SCSMS)

2022

- Updated with additional WFH implications

2021

- Updated to address WFH and Pandemic implications

2020

- Updated to latest mandated requirements and changes to DRP/BCP Template