Compliance Terms and Meanings

Summary

This document provides an overview of key compliance terms and their meanings, focusing on concepts such as audits, assessments, risk management, attestation, certification, benchmarking, and compliance burdens. It explains the importance of understanding these terms for making informed decisions regarding file storage and management solutions like Azure Files and SharePoint. The definitions clarify the roles of independent reviews, regulatory adherence, risk evaluation frameworks, and the administrative challenges organizations face in meeting compliance requirements.

Terms

Audit - An examination performed by an independent third party that verifies the guidelines outlined by experts. Ex: Audits on Infrastructure, DR, Costs & Security

Compliance Audit - is a comprehensive review of an organization's adherence to regulatory guidelines. Independent accounting, security or IT consultants evaluate the strength and thoroughness of compliance preparedness. Auditors review security polices, user access controls and risk management procedures over the course of a compliance audit.

Assessment - The evaluation or estimation of the nature, quality, or ability of someone or something.

Risk Assessment - is the process of identifying variables that have the potential to negatively impact an organization’s ability to conduct business. Some companies use the term audit or review.

Attestation (3rd party) - The acknowledgement of understanding and abidance to policies, procedures, or training.

Certification - An official document attesting to a status or level of achievement.

Benchmarking - Analyzing your data year over year by comparing one's own business processes and performance against the industry standard to reveal compliance program effectiveness and determine needed improvements (Audit scores, Risk scores, Compliance scores)

Compliance Burden - also called regulatory burden, is the administrative cost of a regulation in terms of dollars, time, and complexity.

Risk Assessment Framework (RAF) - is a strategy for prioritizing and sharing information about the security risks to an information technology (IT) infrastructure.

Compliance Risk - is exposure to legal penalties, financial forfeiture, and material loss an organization faces when it fails to act in accordance with industry laws and regulations, internal policies or prescribed best practices.

Compliance - is either a state of being in accordance with established guidelines or specifications, or the process of becoming so

Regulatory Compliance - is an organization's adherence to laws, regulations, guidelines, and specifications relevant to its business. Violations of compliance regulations often result in legal punishment, including federal fines

Corporate Governance - is a term that refers broadly to the rules, processes or laws by which businesses are operated, regulated, and controlled. The term can refer to internal factors defined by the officers, stockholders, or constitution of a corporation, as well as to external forces such as consumer groups, clients and government regulations

Governance, Risk and Compliance (GRC) - is a combined area of focus within an organization that developed because of interdependencies between the three components. GRC software products, available from several vendors, typically facilitate compliance with legal requirements, such as those specified in the Sarbanes-Oxley Act (SOX) or occupational health and safety regulations.

Cyber Security - is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage, or unauthorized access.

Ransomware - is a type of malware (malicious software) distinct from other malware; its defining characteristic is that it attempts to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid.

Internal Control - is a business practice, policy or procedure that is established within an organization to create value or minimize risk

Regulatory Guidelines - Rules established by regulatory authorities that provide direction to those engaged in activities under its jurisdiction. These rules may have the effect of law or merely be recommended procedures.

Compliance Framework - is a structured set of guidelines that details an organization's processes for maintaining accordance with established regulations, specifications or legislation.

Scope of Applicability (SoA) – Scope is an effort to determine the maximum breadth and depth of an assessment, applicability is a concept embedded inside of an organization's agreed-upon scope.

The rules are simple:

1. If even one requirement applies to an item, it is in the assessment scope.

2. If no requirements apply to an item, it is out of the assessment scope.

3. Requirements need not apply to all items in the assessment scope, and that's a good thing.
Example - UofC