ISO 27001:2013
IDENTIFYING APPLICABLE LEGISLATIVE & CONTRACTUAL REQUIREMENTS

DEKRA

"All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization." -ISO 27001:2013 A.18.1.1

by Kim Graham, Senior Business Development Manager

Compliance-Related Evidence

As a Program/Key Account Manager working with several organizations as it pertains to Information Security and Data Privacy Audits, questions regarding supplying clear objective evidence as conforming to this specific requirement arise quite often from our clients.

It is important to note that implementing and maintaining this control to ensure compliance is no easy task, but failing to do so places you at risk of being in noncompliance not only to the ISO 27001:2013 standard, but also to any relevant legislative, statutory, regulatory, or contractual requirements.

Information Security Auditors are not legal advisors or attorneys, but they do play an important role in verifying that evidence exists to support claims of compliance.

Organizations may consider using the following objective evidence for submission to auditors as compliance-related evidence:

- A documented list of customer-specific related requirements from contracts with customers, as it relates to Information Security and Data Privacy (as well as a copy of your current contract)
- A documented inventory of every applicable legislative law and regulation and other Information Security/Data Privacy requirement with which your organization needs to comply
- Emails, agendas, meeting minutes, notes, etc. with Legal or Compliance teams and others with information security or data privacy compliance obligations (such as Procurement, DPO, HR, Finance, IT, Board Members), as it concerns information security in context to compliance objectives (i.e. evidence that management is actively engaged in assessing the extent to which compliance is needed and is aware of the risks of noncompliance)
- Documented plans on how the organization is either meeting or plans to meet requirements (including who is responsible for implementation and when these requirements will be met)
- Internal and external (independent) audit reports/assessments concerning applicable compliance obligations, including detailed corrective actions for any identified nonconformances
- Action item lists with distribution evidence, assigned process owners (including top management), and their current status
- A published Compliance Policy, with supporting guidelines
- Detailed risk assessment(s) of the organization's ISMS

Information Security Auditors provided with this type of objective evidence can make a reasonable determination as to whether an organization is compliant with the applicable requirements and also point out any areas that may require attention or improvement.

Differences Between Statutory, Regulatory, and Contractual Requirements

Statutory obligations are required by law and refer to current laws that were passed by a state or federal government.

Examples of statutory obligations include:

> US Federal Laws
- Children's Online Privacy Protection Act (COPPA)
- The Fair Credit Reporting Act, (FCRA)
- Fair and Accurate Credit Transactions Act (FACTA) - including the "Red Flags" rule
- Family Education Rights and Privacy Act (FERPA)
- Federal Information Security Management Act (FISMA)
- Federal Trade Commission (FTC) Act
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Sarbanes-Oxley Act (SOX)

> State Laws
- California SB1386
- Massachusetts 201 CMR 17.00
- Oregon ORS 646A.622

> International Laws
- Canada - Personal Information Protection and Electronic Documents Act (PIPEDA)
- UK - Data Protection Act (DPA)
- Other countries' variations of Personal Data Protect Acts

Regulatory obligations are required by law but are different from statutory requirements in that these requirements refer to rules issued by a regulating body that is appointed by a state or federal government agency. These are legal requirements through proxy, where the regulating body is the source of the requirement. It is important to keep in mind that regulatory requirements tend to change more frequently than statutory requirements.

Examples of regulatory obligations include:

> US Federal Regulations
- Defense Federal Acquisition Regulation Supplement (DFARS) - NIST 800-171
- Federal Acquisition Regulation (FAR)
- Federal Risk & Authorization Management Program (FedRAMP)
- DoD Information Assurance Risk Management Framework (DIARMF)
- National Industrial Security Program Operating Manual (NISPOM)
- New York Department of Financial Services (NY DFS) 23 NYCRR 500

> International Regulations
- European Union General Data Protection Regulation (GDPR)

Contractual obligations are required duties that each party is legally responsible for in contract agreement with either a customer, service provider, or supplier.

Examples of contractual obligations include:

> Payment Card Industry Data Security Standard (PCI DSS)
> Financial Industry Regulatory Authority (FINRA)
> Service Organization Control (SOC)
> Generally Accepted Privacy Principles (GAPP)
> Data Privacy Agreement (DPA)
> Center for Internet Security Critical Security Controls (CIS CSC)
> Cloud Security Alliance Cloud Controls Matrix (CSA CCM)