Xerox ISO 27001 Security Certifications

Committed to the highest standard of information security

xerox

Xerox ISO 27001Security Certifications

Committed to the highest standard of information security

At Xerox, we have always strived to provide our customers with the strongest information-security infrastructure. That's why, as early as possible, we applied for—and have achieved—the highest international security certification for critical portions of our service environments. These certifications resulted from continuing efforts to secure the integrity of business-critical information for our customers. By conforming to this extremely high standard, we can assure our customers that we are minimizing the risks to these environment. With these certifications in place, our customers can be assured that these Xerox environments have the industry's highest standards for physical security, systems and network security, employment and contract controls, document archiving and destruction.

What is ISO 27001?

ISO 27001 is a standard that ensures security controls are effective, adequate and certified by an international committee. It incorporates a process of scaling risk and valuation of assets with the goal of safeguarding the confidentiality, integrity and availability of written, spoken and electronic information. ISO 27001 specifies requirements for establishing, implementing and documenting Information Security Management Systems (ISMS) and specifies requirements for security controls to be implemented according to the needs of individual organizations.

ISO 27001 defines best practices for information security management processes and is intended to work with other management system standards as a focus on continual improvement processes and on Corporate Governance.

What processes are in place to ensure standards are maintained?

In our certified environments, we consistently refine our processes and risk assessments as part of our continual improvement process. All of our processes and documentation are reviewed by independent auditors, both internal and external.

The audits uncover potential areas for improvement, and provide independent verification of our operations. Unlike other certifications and compliance programs that allow the candidate to specify the applicable controls, ISO 27001 defines a comprehensive list of controls, which each certified environment must comply with.

Ongoing audits enable certification renewal on a periodic basis. The current certificates, as well as the scope of the certifications, are available on request.

ISO 27001 Certification Process:

Achieving ISO 20071 Certification is based on a process approach focusing on the 'PDCA' model: Plan - Do - Check – Act. This requires improved definition and clarification of links between risk assessment, selection of controls and statement of applicability:

- Key Controls include required documented procedures for the control of documents, internal audits, corrective and preventative actions. Records shall be kept of the performance of the process as outlined in establishing and managing the Information Security Management Systems (ISMS) and of all related occurrences of security incidents. Required records also include all education, training, skills, experience and qualifications, management reviews, internal audit results and the results of corrective and preventative actions.
- The Information Security Management Systems (ISMS) Process involves its establishment, implementation and operation, monitor and review and maintenance and ongoing improvement.
- Statement of Applicability encompasses the control objectives, controls and reasons for selection, the control objectives and controls currently implemented and any exclusions and their justifications.

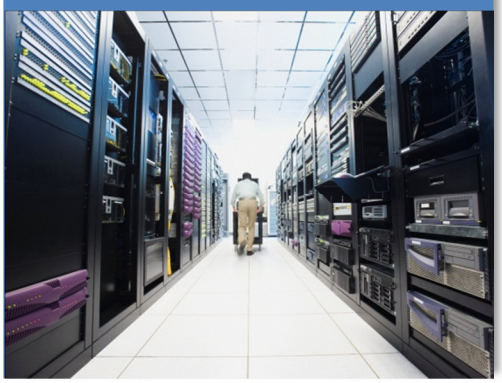
Management Systems:

Management systems are used to develop policies, create objectives and targets using:

- An organizational structure
- Systematic processes and associated resources
- Measurement and evaluation methodology
- A review process to ensure problems are corrected and opportunities for improvement are recognized and implemented when justified.

Key Elements to Management systems include:

- Policy (demonstration and commitment and principles for action)
- Planning (identification of needs, resources, structure, responsibilities)
- Implementation and operation (awareness building and training)
- Performance assessment (monitoring and measuring, handling non
- conformities, audits)
- Improvement (corrective and preventative action, continual improvement)
- Management review



Xerox ISO 27001Security Certifications

Plan-Do-Check-Act Process Model

Plan Phase

- Define the ISMS scope
- Define the ISMS policy
- Define objectives and targets
- Identify assets
- Identify the risks
- Assess the risks
- Select control objectives and controls
- Prepare a Statement of Applicability

Do Phase

- Create a risk plan
- Implement the risk treatment plan
- Implement controls selected to
- meet objectives

Check Phase

- Execute monitoring process
- Conduct internal audits of the Information Security Management Systems (ISMS) at planned intervals
- Undertake regular reviews of the effectiveness of the ISMS
- Review levels of residual risk and acceptable risk

Act Phase

- Implement improvements identified
- Take appropriate preventive and corrective actions
- Communicate the results and actions
- Ensure improvements meet their intended objectives
- Management Commitment
- Business managers need to be seen to be committed (process ownership)
- Expect Chief Executive/Managing Director to demonstrate commitment (Risk Management Decisions)

Security makes all the difference!

At Xerox, we view security as a mandatory requirement for all products and services. We will continue to monitor the ever-changing security landscape, proactively addressing security concerns as they arise.