NAVEX®

Datasheet

27001 Certification with NAVEX IRM™

ISO 27001 specifies the requirements for the policies, procedures and processes that comprise a company's information security management system (ISMS). This international standard was developed to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an ISMS.

ISO 27001 uses a top-down, risk-based approach. Earning certification in this standard is not based on adhering to a set of predetermined rules. Instead, an organization is certified based on a set of controls that are specific to its risks. These controls comprise the company's statement of applicability, a document that ISO auditors will certify an organization against.

ISO 27001 certification is not a one-and-done, checkbox list of requirements. It's an ongoing process of cataloging risks, assessing the severity of risks, applying controls to risks, planning how to remediate risks and providing evidence to auditors that an organization is performing the tasks it identified as important to its risk management. The certification also requires that organizations continually improve their operations from a risk-based perspective.

Traditionally, ISO 27001 documents are stored in network file folders. Tasks are managed through email. And when it comes time for auditors to survey a company's operations, personnel are often sent on a scavenger hunt for the proper documentation. This can lead to companies spending more time on the audit and certification process instead of on operational improvement. It also increases the likelihood of failing an ISO 27001 audit.

This complex matrix can be streamlined using an automated governance, risk management and compliance solution like NAVEX IRM. The solution enables users to link the risks they identify to the policies they create to the processes they administer. This becomes a neatly packaged report that gives auditors the evidence they need to declare an ISMS as ISO 27001 certified.

The NAVEX IRM solution can assist organizations whether they're building an ISMS from the ground up in the hopes of achieving ISO 27001 certification, or they're already certified but want a better way to manage the ongoing audit process. Below are the key areas the solution can streamline the ISO 27001 certification process:

Risk Assessment and Management

The NAVEX IRM solution is capable of conducting any kind of assessment to fit your business needs. The solution also allows you to create new fields and map them to controls, policies and incidents. Develop simple or complex workflow processes to submit, review and approve exception requests with automated alerts, notifications and reminders. You can launch multiple workflows that don't have to be linear.

The solution's risk management function enables users to perform an availability risk assessment, add to and modify their risk registers, and collect data using its survey tool. Risks can be assigned to business units and assigned a risk level, and NAVEX IRM offers multiple risk reporting options.

The NAVEX IRM solution provides a centralized, visible database of IT assets, making it easier to register and assess risks related to applications, software and devices. It automates the process of managing workflows for risk acceptance and approving risk exceptions. The platform also provides the functionality to monitor key performance indicators and track and report key risk indicators.

Audit Management

Audit management encompasses a multitude of tasks, especially for ISO 27001 certification. The NAVEX IRM solution helps users prioritize audit tasks and activities and identify external dependencies for an audit. Organizations can modify audit activities and tasks during audit execution, get project sign-off and track any changes to audit plans post sign-off. The platform shortens the evidence gathering process by allowing business users and auditors to identify process and control owners. Audit tasks can be put into workflow to be completed.

The platform's customized dashboards give users real-time access to data and visibility to audit performance and findings. NAVEX IRM allows users to create customized reports for different recipients, including web-based views of reports. The platform's workflow can facilitate the workpaper/report review and signoff from the project manager or chief audit executive. Audit reports can also be linked to the specific pieces of evidence within those reports.

The bottom line: When an ISO 27001 auditor asks for evidence that you're adhering to a policy, you can click a link on a report housed in NAVEX IRM and the evidence appears. It's stored for future reference, and it can be linked to future activities so you can demonstrate ongoing evolution of your ISMS.

The NAVEX IRM solution's functionality provides the ability to automate the process of issue tracking, by having the platform send notifications regarding inactivity in the audit process, pending risk remediation activities, and finalized audit findings and observations. Nonconformities identified by auditors can easily be tracked enabling an organization to construct corrective action plans to address those findings and manage/track them with workflows. Finally, NAVEX IRM's reporting functionality can produce reports on open, responded, work-in-progress, and closed findings or audit observations.

Policy Management

The NAVEX IRM solution makes management of security policies, IT policies and corporate policies more efficient. The solution can map an organization's ISO 27001 compliance documents to internal controls, and generate workflows that start the policy management review process. It also enables the creation of policy workflows that incorporate IT data, risk data, incident data and other correlated data.

Incident Management

The NAVEX IRM solution provides the means to analyze information security system incidents and manage the appropriate workflows to remediate the risks associated with an incident. Users can create multiple workflows to manage incidents by severity, business unit importance and other criteria.

Business Continuity Management

The NAVEX IRM solution helps businesses create custom continuity plans, manage associated risks and minimize the impact of potential losses. Users can map their business continuity plans to controls within ISO 27001, as well as to other policies, risks, processes and vendors. The platform also enables users to establish workflows to regularly review plans and to allow collaboration between stakeholders to ensure the plans receive all required approvals prior to publishing.

Vendor Management

With the NAVEX IRM solution, users can create third-party policies, tie assessments to those policies, and store and document supplier due diligence and remediation activities. The solution provides the ability to assess the effectiveness of controls and to perform ongoing monitoring at the individual service delivery or contract level.

Manual Methods vs the NAVEX IRM Solution

ISO 27001 certification is a complex process involving risk management, security management, policy management and other disciplines.

Undertaking this endeavor manually using email, spreadsheets and other traditional methods means hunting for information stored in separate systems and/or business units; and even different geographic locations. This makes it difficult to compile, and information becomes documented in an unstructured manner, making it difficult to establish accountability for remediation or mitigation tasks. Furthermore, manual methods cannot be scaled with expansion in stakeholders, regulatory complexities or changing business needs. In short, using traditional methods of documentation, communication, and assessment is inefficient and ineffective.

The NAVEX IRM solution enables a more efficient mechanism to build your ISMS, achieve certification, and streamline the maintenance and process of operating the ISMS on an ongoing basis.

Risk Identification

- Quickly determine and prioritize risks, and maintain a comprehensive risk register to add, track and resolve risks to make timely and accurate decisions.
- Rate inherent risks, link controls to reduce risk and rate residual risk.
- Direct identified risks to specific users for additional analysis via the assignment of tasks with due dates.
- Use assessments to gather, organize, and report on critical risk-related information from the people who work most closely with the associated assets and business processes.
- Identify and justify unmapped controls/risks.

Risk Tracking

- Develop and maintain project schedules for risk tasks, track progress, and hold stakeholders accountable.
- Track exceptions throughout the organization.
- Link risks to specific assets or third-party partners.
- Perform annual risk assessments and review risks on a set schedule using automated workflows to effectively manage risks and maintain compliance.

Policy Development

- Build a policy library and centralize it to provide permission-based access throughout the organization.
- Map policies to regulations, standards, risks and controls.
- Report against which policies address your risk through easy-to-use executive views or dashboards

Incident Preparation and Management

- Use pre-built or create custom incident workflows/processes to track incidents and obtain supporting information.
- Build custom tables to organize information such as incident follow-ups, policy updates, and ISMS meeting notes.
- Collect incident data, store it in a repository with permission-based access, and easily report information to stakeholders.
- Manage remediation through a collaborative workflow engine.

Audit Preparation and Execution

- Gather and store audit evidence and centralize all audit activities into one accessible platform.
- Manage the tracking of audit requests, internal controls and all the communications between team members and external auditors.
- Generate audit and remediation tasks while also providing tools for viewing and sharing audit performance, findings and history.
- Track/manage nonconformities reported by auditors, construct and manage corrective action plans via workflows and reporting.
- Provide auditors the information they want to see in seconds instead of searching for documents on network drives or physical filing cabinets.

For more information on how NAVEX IRM can help you achieve ISO 27001 certification, visit us at www.navex.com