ASCENT
Security Compliance Portal

ISO 27001 Resource Guide

Table of Contents

INTRODUCTION

The ASCENT Portal is a secure cloud-based system of record that supports the security program management needs for organizations of any size, in any industry. As the single source of security and compliance truth, the ASCENT Portal puts everything you need to comply with security control requirements right at your fingertips. From assessment and calendar-driven control task reminders to governance documentation and vendor management, ASCENT automates your compliance process, end-to-end, while delivering real-time status and reports all from a single source.

The ASCENT Portal supports any framework of controls, or multiple frameworks simultaneously – be they defined by regulatory requirements, or internally adopted by your organization. Regardless of the number of security controls your organization has adopted or is required to comply with, the portal manages the entire lifecycle of all controls. While thousands of controls have been developed by our experts to accommodate over forty established controls frameworks, custom or ad-hoc controls developed by your organization can be added anytime.

The ASCENT Portal provides the automation, workflow, and accountability needed for organizations to achieve the goal of continuous compliance. For ISO 27001, you can rest easy knowing that every aspect of control and compliance lifecycle management is effectively managed. This resource guide describes the features and functionality that are provided by the portal to support you in making your ASCENT to compliance with ISO 27001 control requirements.

ASCENT'S HOME PAGE

Upon initial access to the ASCENT Portal, users are presented with their organization's home page within the portal that immediately provides insight into the number of controls that are in place, number of controls not in place, number of controls that are overdue, and the number of upcoming control tasks for the current calendar year.

View Upcoming and Overdue Control Requirements

Gain insight into what is needed to keep compliance on track. Upcoming and overdue controls are listed on the home page to maintain appropriate focus on required activities. The default view is overdue tasks that require immediate attention to maintain compliance. Users can modify views to display controls that are upcoming in the next three days, five days, or the total list of controls assigned to them for the current calendar year. This capability enables managers as well as control owners to plan their schedule according to the upcoming controls they have been assigned. Users can select between viewing this information for the entire organization or choose to only view upcoming and overdue controls that are assigned specifically to them. The data presented from any selected view can be exported on demand for additional planning purposes. If your organization has selected multiple control frameworks with which to comply, these views are automatically adjusted based on the control selected from framework menu.

Reference Library

A reference library is available from the home page that contains information to help ensure your organization is experiencing the most value possible from the ASCENT Portal. The library contains onboarding information, checklists, links to videos, and other useful materials to support your success.

Release Notes

Stay informed with release notes that are published for each ASCENT Portal release. The information contained within release notes describes the latest features and functionality that have been implemented within the portal to improve overall capabilities as well as improve the user experience. ASCENT uses an agile CI/CD development methodology so new releases generally occur every two to three weeks – so stay tuned for updates!

News

Read some of the latest security and compliance updates. The news section contains noteworthy items from sources around the world that are related to security and compliance. The news section is also populated with some of the most popular articles from the ASCENT Portal Blog.

Adding Additional Users

To further support your security and compliance goals, authorized users can submit requests to add additional users directly from the home page. This ensures all appropriate control owners have the access they need within the portal. Automated emails are delivered to new users, as well as the person who requested the new accounts, once a new account is created.

Enhancement Requests

Have an enhancement request? We know a great solution must continue to evolve over time. To support this, users can submit enhancement or feature requests for the ASCENT Portal directly from the home page. While there are similarities in all organizations, there are also differences. This is a fantastic way to ensure your organization's specific needs are addressed. Nearly 10% of the portal's current functionality was developed based on the initial idea or request received from one of our customers over the years. Keep the great ideas coming!

ASSESSMENT & COMPLIANCE

The ASCENT Portal simplifies the security assessment process with dedicated assessment questionnaires for any defined framework of controls. The portal categorizes and defines the prescribed security controls and corresponding compliance requirements. Building on your successful implementation of controls, the portal simplifies the historically challenging process of staging your compliance program while providing field-proven guidance and real-time insights on your overall security and compliance status.

Dashboards

Real-time dashboards provide graphical representation of the overall status of your security program. Dashboards update automatically after any control is completed or becomes "overdue." Dashboards display the overall compliance score, on a scale of 0 to 100; monthly score trends for the previous twelve months, along with that average; and control status breakdown that identifies the percentage of controls that are in place, not in place, and those deemed to be not applicable.

Individual control family scores that make up the overall compliance score are displayed that provides more granular insight based on individual sections of your control framework. All of the information presented within dashboards is automatically modified based on the framework menu selection if your organization has adopted more than one framework of controls.

Security Control Assessment Questionnaires

ASCENT Portal assessment questionnaires begin the lifecycle management of each defined control requirement. Once an initial assessment questionnaire is completed, your organization never again has to start an internal security control assessment, or external assessment preparation, from the beginning. Your results are maintained in perpetuity and automatically updated based on implementing new controls, the re-verification of existing controls, or when re-verification of a control becomes overdue.

Completing assessment questions is a straightforward process. Recommended remediation steps and artifact examples are included for control questions within the portal, along with a list of all artifacts that have been uploaded to date. Users also have the ability to add notes for any control. Notes are stored within the portal for reference and can be emailed from the portal to any user when the note is created. Additionally, users can review the timeline for each control that contains all actions performed for a specific control, by whom the action was performed, along with a date and time stamp for each timeline entry. Lastly, the completion status showing the percentage of questions that have been completed for each control family is graphically displayed for easy reference, tracking, and prioritization.

Once assessment questions are answered and any supporting materials have been uploaded, the portal maintains this information in perpetuity. Future assessments require only the current status of controls to be review. This saves countless hours during recurring control reviews that your organization performs.

Security & Compliance Calendar

Keep controls current. Assessing the effectiveness of your security program once a year is not enough. This can lead to a false sense of protection throughout your organization. The Security and Compliance Calendar presents pre-scheduled due dates for all in-scope security controls throughout the calendar year. This allows your organization to review and assess small portions of your security program each

month versus assessing all controls and associated artifacts in a one to two-week period. Maintaining security controls in line with the defined schedule helps ensure controls remain effective, evidence and artifacts remain current, and your organization is always ready for any assessment, audit, or examination of controls.

Email reminders are automatically delivered to control owners when a control is assigned to them. Based on the calendar, email reminders are delivered when the due date for controls is within five days, when the due date is within one day, and when the control has been successfully completed. If desired, the same emails that are delivered to the control owner can also be delivered to the administrator(s) of the ASCENT Portal for your organization. Generally, this is the CISO, CIO, or other member of management.

ASCENT Control Evidence Documents (CEDs)

Evidence collection is a necessity when it comes to proving that your security controls have been implemented and are operating effectively. While necessary, this can be a tedious, time-consuming event. This repetitive exercise is especially difficult without having a defined process in place to collect, manage, and present control evidence for assessments, audits, or exams.

The ASCENT Portal solves this potentially frustrating issue with Control Evidence Documents, or CEDs. An ASCENT CED is evergreen artifact that contains the control description, communicates how your organization satisfies the control, and lists any reference materials for the control. A CED template is included for ***every*** control within the ASCENT Portal, whether your control framework has 100 or 1,000 controls. Once CEDs are completed, the time required to compile and provide control evidence is a fraction of what it would be without this easy-to-use solution. Lauded by assessors, CEDs save time for your organization as well as those reviewing control evidence which leads to reduced audit timelines and preparation costs.

One of the most favorable benefits of using CEDs is their ability to be re-used month after month, year after year, and audit after audit. Once a CED has been created for a specific control, verifying that the documented evidence is still accurate is the only requirement for re-use. Occasionally, a new screenshot or document reference may be required, but the amount of time to complete the gathering of evidence continues to be reduced exponentially. The ASCENT Portal ensures you never have to start evidence collection from scratch again.

Artifact Library

All artifacts and supporting documentation that have been uploaded to serve as evidence of control effectiveness, including CEDs, are automatically added to the Artifact Library. This is performed by the portal; no manual activity is required. A report listing all artifacts that have been uploaded to the library can be generated on demand anytime. The library contents can also be exported at any time. Further, limited read-only access to the library can be provided to auditors, examiners, or assessors to support reviews of your security program.

Risk Assessments

The ASCENT Portal's Risk Assessment functionality allows cross-functional stakeholders within your organization to complete a detailed risk assessment. Once the risk assessment is completed, the annual requirement of completing subsequent risk assessments is easily managed by making only necessary updates based on changes to your organization, newly defined threats, or completed mitigation and remediation efforts.

Our risk assessment addresses environmental risks, human-made risks, business risks, and IT risks. Each risk assessment question managed by the portal records entries for the potential financial impact, operational impact, strategic impact, legal impact, and reputational impact that is estimated for your organization. Once appropriate values have been entered, the severity for each risk item is automatically calculated by the portal.

After the initial risk assessment has been completed, the ASCENT Portal tracks whether or not the identified risks have been determined to be acceptable by your organization. The portal also records any comments entered for identified risks, to whom remediation or mitigation activities are assigned, the estimated remediation dates, the status of remediation, and date the risk was remediated. All of this information is available via a Risk Assessment Report that can be generated on demand at any time.

Enterprise Dashboards

Organizations have the option to implement multiple instances of the portal for various locations, business units, or affiliates. This is common for organizations that are made up of different companies or smaller, autonomous organizational units.

Enterprise dashboards allow organizations to see the security and compliance status for each tenant as well as the combined average of the overall organization.

Personnel Acknowledgements

The portal provides the ability to assign and track acknowledgement requirements made by personnel for specific materials. This may include policies, acceptable use requirements, access agreements, or your organization's code of conduct that are required to be read and acknowledged on a regular basis. Once assigned, users are notified of the requirement and the portal tracks completion. Reports can be generated at any time to demonstrate compliance status.

SECURITY PROGRAM GOVERNANCE

To support the adoption of regulatory control requirements and security best practices, the ASCENT Portal provides all of the policies, plans, and procedures organizations need to effectively communicate security control requirements to personnel. All governance documents are customizable to support branding by your organization and can be tailored to meet your specific needs.

Policies, Plans, and Procedures

Out team of security experts have designed security policies, plans, and procedures to effectively document and communicate the control requirements for your security program. These governance documents are benchmarked against the specific framework selected and published to your portal. Content can then be customized over time to continually meet the evolving needs of your organization.

Exception Management

One of the procedures provided by the ASCENT Portal is the Exception Management Procedure. This procedure defines the process of requesting, approving, and tracking temporary control exceptions that may occasionally be required. In addition to the procedure, the exception management process workflow is contained within the ASCENT Portal and allows exception requests to be submitted, approved, or denied. Remediation can also be tracked directly within the portal.

Incident Response

A comprehensive Incident Response Plan is included and is accessible from the governance page. The ASCENT Portal also provides incident response workflow management to support the completion of appropriate response activities. The workflow built into the portal addresses the following:

Step 1: Assigning an Incident Handler

Step 2: Capturing details about how the incident was reported

Step 3: Documenting preliminary details about the incident

Step 4: Classification of the suspicious activity

Step 5: Recording device and network information related to the incident

Step 6: Documenting the source of the incident

Step 7: Containing the incident

Step 8: Incident eradication

Step 9: Incident recovery

Step 10: Conducting post-incident lessons learned meetings

Incident Call Notes: Documenting action items and results that are identified during incident calls throughout the response process.

Incident reports can be generated at any time and distributed to ensure appropriate stakeholders are kept informed throughout the entire incident response process.

Security Program Summary

A customizable Security Program Datasheet provides external audiences with an overview of your security program. Appendices of this document include the table of contents for your security policies and Incident Response Plan. This is important as your policies may be classified as "Internal Use Only," while the Incident Response Plan is likely to be classified as "Confidential." Organizations should not classify and protect these documents appropriately, then provide them to anyone who asks for them without any consideration being given to their release. This datasheet can be a valuable tool when responding to inquiries about the overall security program.

BUSINESS CONTINUITY

With the ASCENT Portal, you have a solution to help manage business continuity. The portal includes customizable business continuity and disaster recovery plans, contingency planning guidance, and business impact analysis so you can ensure that you not only meet compliance requirements for planning, but support your business with operational resilience in the event of an unexpected outage event.

Strategic Plan

A customizable Business Continuity Strategic Plan is provided that includes the overall plan for maintaining contingency planning documentation, implementing testing schedules, and identifying critical operations throughout your organization.

BC and DR Plans

Access business continuity and disaster recovery plans to customize your actin plan to keep business operations running. The templates include Business Impact Analysis processes for prioritizing information assets and services to support the prioritization of recovery needs.

Call Trees

Contact information for personnel with business continuity or disaster recovery responsibilities can be maintained within call tree templates that are available on the business continuity page.

Test Plans and Test Reports

Customizable continuity and recovery test plan and report templates are available for documenting the steps planned for each testing exercise along with the results.

No Impact from Outages

As a cloud-based solution, the ASCENT Portal provides continuous access to critical business continuity documents for your personnel even if an outage occurs that impacts local storage devices.

CYBERSECURITY

The cybersecurity page provides the ability for security monitoring tools that have been implemented within your environment to publish recurring reports directly to the portal for action, reference, monitoring, and to demonstrate compliance with associated monitoring controls. This module also contains pre-built repositories for cybersecurity monitoring plans, network diagrams, and vulnerability registers.

VENDOR MANAGEMENT

Perform your vendor due diligence and supply chain risk management with seamless efficiency. The ASCENT Portal provides dedicated links for vendor due diligence questionnaires to be completed directly in the portal, minimizing tedious staff management and coordination actions.

Preliminary Assessments for Risk Ranking Vendors

Categorize vendors and suppliers based on the risk ranking results of a preliminary assessment. These short, effective, and efficient questionnaires are automatically created for each vendor that is added to the ASCENT Portal. Once completed by your internal resources, the results of preliminary assessments are used to risk-rank vendors and suppliers to determine if additional due diligence requirements are appropriate or required.

Due Diligence Assessments

Depending on the risk level defined by the preliminary assessment, due diligence questionnaires may be required for critical vendors and suppliers. Due diligence assessment questionnaires are automated, with links that can be sent to vendors and suppliers for completion directly in the portal – no more spreadsheets!

Vendors and suppliers also have the ability to upload appropriate artifacts to support the responses they provide during the due diligence assessment process. All vendor-specific artifacts are contained within their assigned folder for review and future reference. Overall and individual vendor due diligence status reports are available on demand with a click of a button.

Contract Library

Contracts can be uploaded to the ASCENT Portal for each vendor that is added. Contract information captured by the portal includes contract name, service description, start date, end date, relationship manager, and contract status. This functionality enables your organization to manage contract renewals, expirations, and cancellations within predefined time requirements.

SECURITY AWARENESS TRAINING

Defend your organization with employees that are trained on security best practices and regulatory requirements for protecting the confidentiality, integrity, and availability of information, systems, and other assets. ASCENT provides a training program with simplified management for annual, new hire, and role-based training.

Recurring Awareness Training

Deliver recurring security training for all personnel throughout your organization for spotting security breaches, complying with security policy requirements, using technology best practices to keep cyberthreats at bay, and myriad of other topics.

New Hire Training

Provide required training for new hires as they are onboarded, or within their first 30 days of being hired. New hire training modules are available to ensure newly onboarded personnel become familiar with requirements for protecting information assets, complying with organization-defined controls, and other appropriate information that applies to new personnel.

Functional Role-Based Training

Role-based training is available for key roles associated with the security program. Your organization can provide training for specific roles such as incident response team members, personnel responsible for business continuity, IT Administrators, HR personnel, and Executive Leadership.

Training Reports

Ensure employees complete required training requirements with reporting that ensures your organization has prepared employees that remain knowledgeable and vigilant. Training reports help protect organizations by serving as artifacts that show individuals have been appropriately trained. It is difficult for unauthorized or potentially nefarious activities to be defensible if the organization has a record of training employees against such behavior. Training records also serve as great control evidence for external assessments and audits.

SECURITY PROGRAM REPORTING

The ASCENT Portal provides easy-to-understand reports that demonstrate the current security program status, compliance status, control gaps, and overdue control tasks. Weekly status reports are automatically generated, published to your portal, and delivered via email to defined personnel within your organization. Complete security control assessment reports can be generated on demand anytime.

The reporting page also serves as a repository for your organization to maintain corrective action plans, metrics, and external audit reports. This enables these items to be stored securely and made available to all appropriate personnel for action, reference, and control compliance.

USER SUPPORT

Get the support your need when you need it. Each section of the ASCENT Portal contains a dedicated user guide with detailed instructions for performing actions within that section. Plus, our customer support team is available twenty-four hours a day to respond to any questions, operational opportunities, or other related support inquiries. Staffed 100% with full-time ASCENT Portal employees, our global support team ensures all requests are managed by the experts that have the most knowledge to reduce resolution times and provide the best available support.

PRICING & RETURN ON INVESTMENT (ROI)

ASCENT Portal Pricing

Pricing for the ASCENT Portal in simple and straightforward. Our transparent pricing consists of a monthly subscription cost plus a user license cost. The pricing below includes all of the features and functionality included in this resource guide.

ASCENT Portal SaaS Subscription: $500 per month

Plus:

1-50 Users: $14 per user, per month

51-500 Users: $10 per user, per month

501+ Users: $5 per user, per month

(Pricing is subject to change.)

Return on Investment

Let's take a look at the return on investment you can expect as a result implementing the ASCENT Portal for your organization. These ROI estimates are based only on salary estimates for the number of full-time employees (FTEs) that would no longer be dedicated to security program administration. Factors such as the cost of providing employee benefits, bonuses, time taken away from other projects, and other costs are not included in these ROI figures. Just focusing on employee salaries makes the ASCENT Portal an easy decision for organizations based on the ROI figures alone, which are listed on the next page.

For these ROI calculations, the following assumptions were made:

- The average annual salary for FTEs administering the security program for a small organization is $100,000.
- The average annual salary for FTEs administering the security program for a mid-sized organization is $120,000.
- The average annual salary for FTEs administering the security program for a large organization or enterprise is $140,000.
- All ASCENT Portal functionality is currently being performed, or is planned for implementation, using manual processes.

ROI and Savings Details:

For a small organization with 25 portal users:

- ROI = **959%**
- Reduction/Avoidance of 1.2 FTE requirements = **$120,000 savings**
    - FTEs needed without ASCENT Portal: 2.7
    - FTEs recommended with ASCENT Portal: 1.5

For a mid-sized organization with 250 portal users:

- ROI = **1,017%**
- Reduction/Avoidance of 3.35 FTE requirements = **$402,000 savings**
    - FTEs needed without ASCENT Portal: 7.25
    - FTEs recommended with ASCENT Portal: 3.9

For a large organization or enterprise with 1,000 portal users:

- ROI = **1,321%**
- Reduction/Avoidance of 6.7 FTE requirements = **$938,000 savings**
    - FTEs needed without ASCENT Portal: 13.25
    - FTEs recommended with ASCENT Portal: 6.55

Ready
to get started
with your ASCENT?

Visit ascent-portal.com to schedule
a demo focused on making the ASCENT to
your security and continuous compliance goals.

This document and all of the information contained in it, including without limitation all text, data, graphs, and charts (collectively, the "Information") is the property of Ascent Portal, LLC. ("Ascent"). The user of the Information assumes the entire risk of any use it may make or permit to be made of the Information.

ASCENT MAKES NO EXPRESS OR IMPLIED WARRANTIES OR REPRESENTATIONS WITH RESPECT TO THE INFORMATION AND EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES (INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF ORIGINALITY, ACCURACY, TIMELINESS, NON-INFRINGEMENT, COMPLETENESS, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE) WITH RESPECT TO ANY OF THE INFORMATION.

Without limiting any of the foregoing and to the maximum extent permitted by law, in no event shall Ascent have any liability regarding any of the information for any direct, indirect, special, punitive, consequential (including lost profits), or any other damages even if notified of the possibility of such damages. The foregoing shall not exclude or limit any liability that may not by applicable law be excluded or limited.