



ASCENT Portal User Guide 2024



Table of Contents

Chapter 1 – Introduction

- What is ASCENT Portal?
- What are the benefits of using ASCENT Portal?
 - How the ASCENT Portal can assist your security posture and corporate roadmap
- Additional services we provide
- Who is ASCENT Portal designed for?
 - o Individuals
 - Industries
- Frameworks provided
- Frequently Asked Questions (FAQ)

Chapter 2 – Getting Started

- Getting signed up and logged in for the first time
- How to reset your password
- How to get support for the Portal
- Glossary
- Dashboard
- Notifications and Alerts to Help Manage Controls
- Calendar
- Artifacts
 - How to upload artifacts
 - How to delete artifacts
 - Viewing and downloading all artifacts
- Reports
 - Automated weekly status reports
 - How to find the automatically generated reports
 - Generating framework reports manually

Chapter 3 – Using the Portal – General

- Types of Access
- Adding New Users to the Portal
- Assigning and Managing Controls
 - Assigning controls
 - Managing controls for the organization
 - Managing controls assigned to you, an admin
 - Managing controls assigned to you, a user
 - Alerts to help manage controls
 - Viewing and managing your to do list of controls
- Assigning Frameworks

- Governance
 - Policies
 - Templates
- Incident Response

Chapter 4 – Using the Portal – MSP

- Navigating the admin section
- Editing tenant details
- Adding users to a tenant
- Assigning frameworks to a tenant
- Deactivating a framework for a tenant
- Setting access types for a new user within a tenant
- Exporting tenant details in Excel format
- Viewing a compliance score of a tenant
- Creating a summary of compliance scores for all tenants
- Setting overdue control automatic email frequency for a tenant
- Adding an internal/external auditor to the Portal



Chapter 1: Introduction

What is ASCENT Portal?

We've designed the ASCENT Portal to take the guesswork out of cybersecurity and give you back the control and clarity you need. The best part is you do not need to be an IT expert to manage your ASCENT Portal.

ASCENT Portal provides an automated governance, security, and compliance platform that simplifies risk management and streamlines compliance. With the ASCENT Portal's real-time compliance scoring, you can easily monitor your compliance posture and immediately identify areas of improvement, all while ensuring team accountability and reducing the compliance workload.

ASCENT Portal identifies the controls you need to have in place, allows you to assign tasks and due dates, schedules the tasks throughout the year for a manageable cadence of work, and automatically communicates with your insurance broker when there are potential risks of not having a control up to date.

We build out the entire framework and automation for you, so it is easy to remain in compliance throughout the year and stay in touch in real-time with your insurance broker.

What are the benefits of using ASCENT Portal?

ASCENT Portal is a Security Compliance Portal that offers various benefits to organizations in managing and ensuring compliance with security standards and regulations.

In under 3 minutes, the ASCENT Portal can calculate your security compliance score. This score can be used to help establish a cyber security threshold that is customized to your company's need.

Here are some key benefits of the ASCENT Portal:

Achieve trust and certainty – By automating compliance and simplifying risk management, you can better certify the trust that your clients place in you.

Save time and resources – Our platform and services streamline the compliance process, freeing up your team to focus on other important business activities.

Stay ahead of compliance requirements – Our solution helps you stay up to date with ever-changing compliance requirements, so you can avoid costly fines and penalties.

Centralized Management - ASCENT Portal provides a centralized platform to manage and monitor security compliance activities of your organization. This streamlines processes and makes it easier to oversee the entire compliance landscape.



Efficient Tracking – ASCENT Portal allows for efficient tracking of compliance status', helping organizations keep up-to-date records of adherence to security policies and regulations.

Automation of Compliance Checks – Automation features within the Portal can streamline the compliance checking process, reducing manual efforts and minimizing the risk of human error.

Real-time Monitoring - Real-time monitoring capabilities enable organizations to promptly identify and address any non-compliance issues, enhancing overall security posture.

Document Management – ASCENT Portal includes document management features, facilitating the storage, retrieval, and organization of relevant compliance documentation and artifacts.

Auditing and Reporting – Robust auditing and reporting functionalities in ASCENT Portal help organizations generate comprehensive reports for internal reviews, audits, or regulatory assessments, demonstrating compliance efforts.

Collaboration and Communication - ASCENT Portal often supports collaboration among team members, fostering effective communication and coordination in achieving and maintaining compliance.

Customization and Flexibility – ASCENT Portal offers customization options to tailor compliance processes to the specific needs and requirements of the organization by providing an option to upload Customized framework.

Notifications and Alerts – ASCENT Portal can provide automated notifications and alerts for upcoming compliance deadlines, ensuring proactive measures to address potential issues.

Scalability – ASCENT Portal is a scalable platform that can accommodate the growing needs of an organization, making it suitable for businesses of various sizes and industries.

Enhanced Security Culture – By promoting awareness and adherence to security policies contributes to fostering a culture of security within the organization.

Additional services we provide

Ascent Security Services - Onboarding & Project Services

- Ascent BaseOnboarding
 - QuickStart of Ascent Portal services for an organization covering the basics from portal onboarding to selection of frameworks of control and configuration of 3rd party plugins.
- Ascent ProOnboarding S
 - Advanced onboarding service that guides the customer through baseline assessment of a simple framework, identification of controls that exist, are missing and/or applicable to the organization. Ascent ProOnboard service walks the organization through control assignment and establishing timelines for controls within security frameworks.



- Ascent ProOnboarding M
 - Advanced onboarding service that guides the customer through baseline assessment of a moderate framework, identification of controls that exist, are missing and/or applicable to the organization. Ascent ProOnboard service walks the organization through control assignment and establishing timelines for controls within security frameworks.
- Ascent ProOnboarding E
 - Advanced onboarding service that guides the customer through baseline assessment of a extensive framework, identification of controls that exist, are missing and/or applicable to the organization. Ascent ProOnboard service walks the organization through control assignment and establishing timelines for controls within security frameworks.

Add-On: Ascent ProOnboard

- Ascent Cyber Insurance Control Mapping
 - The Cyber Insurance Control Mapping service is an add-on to the Base and ProOnboard service, assisting an organization with the discovery of required controls from their cybersecurity policy and mapping those controls in the GRC portal, helping the end client understand the requirements of their own cybersecurity insurance policy.
- Ascent Cyber Insurance Assessment
 - The Cyber Insurance Assessment provides an analysis of a customer's Cyber Insurance Policy and identifies the controls required for the policy. A remediation plan is crafted to provide guidance on reconciliation of the carrier's requirements to the organization's controls. Additionally, assistance is provided filling out the following year(s) of the cybersecurity insurance application.
- Ascent Cyber Insurance IT Audit
 - The Cyber Insurance IT Audit is a 1-day add-on to the ProOnboard service to assist an organization with the discovery and validation of IT assets to validate the controls needed for Cyber Security requirements.

Ascent Security Services - Onboarding & Project Services

- Ascent PartnerSuccess Services
 - QuickStart of Ascent Portal services for Partner organization covering the basics from portal onboarding to selection of frameworks of control and configuration of 3rd party plugins. Direct participation with identifying initial prospects and assisting partner with literature. Includes assistance/execution of pitches for first 5 customers.
- Ascent White Label Services
 - Personalization of the Ascent portal to be branded with company's image including Logo and white labeled URLs. Rebranding of Ascent Portal to Desired Logo/Colors
- Ascent WISP Workshop
 - the WISP Workshop Package is an all-in-one solution designed to uplift and organization's information security posture. This service is tailored to provide your team with the tools, knowledge, and support needed to fortify cybersecurity defenses. This service is ideal for organizations looking to establish a solid foundation in information security and take proactive steps towards continuous improvement of their program. Includes 2x Penetration tests and 1 license of Ascent portal for 1 year.
- Ascent Frameworks S



- The Simple Custom Framework Development service is designed to cater to organizations seeking to establish a specialized or custom-tailored security control framework. This service is ideal for businesses that require a personalized approach to security and those that must abide by industry or vendor-specific risks and compliance requirements unique to their operations.
- Ascent Frameworks M
 - The Moderate Custom Framework Development service is designed to cater to organizations seeking to establish a specialized or custom-tailored security control framework. This service is ideal for businesses that require a personalized approach to security and those that must abide by industry or vendor-specific risks and compliance requirements unique to their operations.
- Ascent Frameworks E
 - The Extensive Custom Framework Development service is designed to cater to
 organizations seeking to establish a specialized or custom-tailored security control
 framework. This service is ideal for businesses that require a personalized approach to
 security and those that must abide by industry or vendor-specific risks and compliance
 requirements unique to their operations.
- Client Baseline Security Assessment
 - A review of clients present security posture and adherence to cybersecurity best practices.
- Ascent BaseOnboarding + Cybersecurity Insurance Control Mapping + Ascent PartnerSuccess Services
 - Popular Bundle of Services for Partners Beginning with Ascent. Includes Base Onboarding covering the basics from portal onboarding to selection of frameworks of control and configuration of 3rd party plugins, adds one Cyber Insurance policy control mapping service to assist an organization with the discovery of required controls from their cybersecurity policy and mapping those controls in the GRC portal, and finally including assistance/execution of pitches for first 5 customers to begin building partner revenue quickly.

Ascent Security Services - Operations

- Ascent Compliance Builder S
 - Advanced onboarding service that guides the customer through baseline assessment of an Simple framework, identification of controls that exist, are missing and/or applicable to the organization. Ascent ComplianceBuilder service walks the organization through control assignment and establishing timelines for controls within security frameworks.

• Ascent Compliance Builder – M

- Advanced onboarding service that guides the customer through baseline assessment of an moderate framework, identification of controls that exist, are missing and/or applicable to the organization. Ascent ComplianceBuilder service walks the organization through control assignment and establishing timelines for controls within security frameworks.
- Ascent Compliance Builder E
 - Advanced onboarding service that guides the customer through baseline assessment of an Extensive framework, identification of controls that exist, are missing and/or applicable to the organization. Ascent ComplianceBuilder service walks the organization through control assignment and establishing timelines for controls within security frameworks.



Ascent Integrated Penetration Testing Services

• Integrated penetration testing services for partners and clients, with results automatically populating relevant control questions from desiganted clients or partner control families

Ascent Security Services - Response & Remediation Services

- Ascent Assess
 - The Security Assessment is designed to evaluate and enhance an organization's governance, risk, and compliance (GRC) program, providing a robust assessment regarding cybersecurity risks. The service aims to provide a holistic assessment of the organization's cybersecurity readiness, ensuring that it is well-prepared to manage and mitigate cyber risks, and is aligned with best practices in governance, risk management, and compliance.
- Ascent Breach Response Services
 - The Cybersecurity Breach Response service is a comprehensive solution designed to assist organizations in the immediate aftermath of a security breach. Recognizing the critical nature of these incidents, our service is focused on rapid response, containment, and recovery, ensuring minimal impact on business operations. Our team of experienced cybersecurity professionals is equipped to handle various types of breaches, providing expert guidance and support throughout the incident including engagement with a 3rd party forensics firm. Sold on a per hour basis, 10 hour minimum.

Ascent Managed Security Operations Center Services

- Ascent Essential Managed Security Operations Center Services
 - XDR SIEM/SOC Essential Base Package/Month, includes 75 IPs
- Ascent Standard Managed Security Operations Center Services
 XDR SIEM/SOC Standard Base Package/Month, includes 75 IPs
- XDR SIEM/SOC Premium Base Package/Month, includes 75 IPs
 - Whitehat XDR SIEM/SOC Premium Base Package/Month, includes 75 IPs
- XDR Additional Site
- XDR 200 IP Block Upgrade
- Ascent XDR 25 IP Block Upgrade
 - o Add-on 25 IP Block Upgrade Building Block to Meet Client IP Address Count

XDR Cyber Platform Setup

- XDR SIEM/SOC Essential One Time Setup Fee
- XDR SIEM/SOC Standard One Time Setup Fee
- XDR SIEM/SOC Premium One Time Setup Fee

Whitehat XDR Cyber Platform Additional Site Setup

- XDR Essential Additional Site One Time Setup Fee
- XDR Standard Additional Site One Time Setup Fee
- XDR Premium Additional Site One Time Setup Fee
- Ascent Vendor Due Diligence Services
 - A Comprehensive Vendor Due Diligence Program is an essential service for businesses that rely on a network of vendors for their operations. This service is designed to assess, stratify,



and manage the risks associated with each vendor, ensuring that the business relationships enhance, rather than endanger operational integrity.

• Ascent Human Risk Management Services

Ascent Human Cyber Risk Management Services - "HRM as a Service"

- Phising Simulation & Training 1 User/Yr
 - Enterprise Smishing, Vishing, and Phishing Training
- CyberEscape Online 1 user/Yr
 - Immersive, Teams-Based CyberEscape Online Experience a fun, immersive, and interactive cybersecurity training program that's 16X more effective than standard training.
- Unify Insights: Human Risk Management Platform
 - Proactively quantify your organization's vigilance, engage your workforce, and measure human risk.
- Human Risk Management Operations Center (HROC)
 - It's one pane of glass that identifies your riskiest individuals, helps you efficiently plan next actions, and measures the impact of improving human behavior.

Who is ASCENT Portal designed for?

Security compliance is designed for various stakeholders across different industries who are responsible for ensuring that an organization's information systems, processes, and practices adhere to established security standards, policies, and regulations. The primary audience for security compliance includes:

Individuals

IT Professionals – System administrators, network administrators, and other IT professionals play a crucial role in implementing and maintaining security controls to ensure compliance.

Security Officers and Managers - Individuals responsible for overseeing the organization's security strategy and managing security teams are key stakeholders in the compliance process.

Compliance Officers - Compliance officers or specialists are dedicated professionals who focus on ensuring that the organization complies with relevant laws, regulations, and industry standards.

Risk Managers - Professionals involved in assessing and managing cybersecurity risks are integral to the compliance process, identifying potential threats and vulnerabilities.

CPA, Legal and Regulatory Affairs - CPAs, legal professionals and regulatory affairs teams ensure that the organization complies with relevant laws and regulations, helping to mitigate legal risks. **Executives and Leadership -** C-level executives and organizational leaders have a vested interest in maintaining a secure and compliant environment to protect the company's reputation and financial wellbeing.



Auditors and Assessors - Internal and external auditors, as well as third-party assessors, play a critical role in evaluating and verifying the organization's compliance with security standards.

Employees - All employees contribute to security compliance by following policies and procedures, participating in training, and being aware of their role in maintaining a secure environment.

Industries

A security compliance Portal can be valuable across various industries to ensure that organizations adhere to the necessary security standards, regulations, and best practices. Here are some industries where a security compliance Portal can play a crucial role:

Finance and Banking: Given the sensitive nature of financial data, compliance is critical in the finance sector. A security compliance Portal can help ensure adherence to regulations such as PCI DSS (Payment Card Industry Data Security Standard) and others.

Healthcare: The healthcare industry deals with highly sensitive patient information. Compliance with regulations like HIPAA (Health Insurance Portability and Accountability Act) is essential to safeguard patient data.

Government and Public Sector: Government agencies and public sector organizations handle a vast amount of sensitive data. Compliance with government regulations and security standards is imperative to protect citizen information.

Information Technology (IT) and Software Development: IT companies and software developers must adhere to various security standards to protect customer data and intellectual property. Compliance with standards such as ISO 27001 is common.

E-commerce: Online retailers process a significant amount of customer information and payment data. Compliance with standards like PCI DSS is crucial to ensure the security of online transactions.

Energy and Utilities: Companies in the energy sector may need to comply with regulations specific to critical infrastructure protection. Ensuring the security of systems is vital to prevent disruptions and potential cyber threats.

MSP's - MSPs managing multiple clients with diverse security requirements. A centralized Portal allows them to oversee and manage the security compliance of all clients from a single platform.

Telecommunications: Telecommunication companies deal with vast amounts of customer data and must comply with regulations to ensure the privacy and security of communication services.



Education: Educational institutions handle student records and sensitive research data. Compliance with regulations such as FERPA (Family Educational Rights and Privacy Act) is essential to protect student information.

CPA Firms: Implementing a Security Compliance Portal for CPA (Certified Public Accountant) firms is crucial to ensuring the protection of sensitive financial data, maintaining client trust, and complying with industry regulations.

Frameworks provided

We provide over 25 frameworks and can also add a custom designed framework to your Portal upon request. Below is our current standard list of frameworks.

AICPA TSC 2017 CIS CSC v8.0 **COBIT 2019** COSO v2017 CSA CCM v4 GAPP ISO22301 v2022 ISO22302 v2013 ISO27001 v2013 ISO27001 v2022 ISO270017 v2015 **NIST Privacy Framework** NIST 800-53 NIST 800-82 NIST 800-161 NIST 800-171 PCIDSS v3.2 US CMMC 2.0 Level 1 US CMMC 2.0 Level 2 US CMMC 2.0 Level 3 **US FEDRAM** HIPPA – HICP SOX US TX-RAMP Level 1 US TX-RAMP Level 2 US TX- Cybersecurity act **US Privacy Shield US FERPA** WISP Framework



Frequently Asked Questions (FAQ)

What is ASCENT PORTAL?

ASCENT Portal provides an automated governance, security, and compliance platform that simplifies risk management and streamlines compliance.

With the ASCENT Portal's real-time compliance scoring, you can easily monitor your compliance posture and immediately identify areas of improvement, all while ensuring team accountability and reducing the compliance workload.

ASCENT Portal identifies the controls you need to have in place, allows you to assign tasks and due dates, schedules the tasks throughout the year for a manageable cadence of work and automatically communicates with your insurance broker when there are potential risks of not having a control up to date.

We build out the entire framework and automation for you, so it is easy to remain in compliance throughout the year and stay in touch in real-time with your insurance broker.

How does ASCENT Portal help you to remain in compliance?

We help you maintain adherence to industry standards by helping you choose which frameworks to build into your Portal.

Each framework has several controls, or assignments, that need to be completed. The Portal allows you to assign each of the controls to an owner and set a due date for each.

The owner will be automatically reminded by the Portal of upcoming due dates to help ensure everyone stays on track.

The Portal also pre-plans assignments to control owners throughout the year so it's a manageable workload for all stakeholders.

How is the Portal secure?

All data transmitted between your device and our servers is encrypted using industry-standard protocols. This ensures that your sensitive information remains confidential during transit.

ASCENT Portal incorporates robust access controls, user authentication is carefully managed, and access permissions are assigned based on roles, ensuring that users only have access to the information necessary for their responsibilities.

We conduct regular security audits and 3rd party assessments to identify vulnerabilities and address potential risks promptly. This proactive approach helps us stay ahead of emerging security threats.



To prevent data loss and ensure business continuity, we implement regular data backups. In the event of any unforeseen incidents, our recovery processes are in place to minimize downtime and restore services swiftly.

We believe in transparency when it comes to our security practices and regularly communicate with our users about security updates, incidents (if any), and best practices.

Your security is our priority, and we are dedicated to maintaining a secure and compliant environment for your data.

What industries does ASCENT Portal cater to?

ASCENT Portal caters to any industry that must comply with security policies or controls. Here are some examples of the industries we serve:

- Finance and Banking
- Healthcare
- Government and Public Sector
- Information Technology and Software Development
- E-commerce
- Energy and Utilities
- MSP's
- Telecommunications
- Education
- CPA Firms

What frameworks does ASCENT Portal provide?

We provide over 25 frameworks and can also add a custom-designed framework to the Portal upon request:

- AICPA TSC 2017
- CIS CSC v8.0
- COBIT 2019
- COSO v2017
- CSA CCM v4
- GAPP
- ISO22301 v2022
- ISO22302 v2013
- ISO27001 v2013
- ISO27001 v2022
- ISO270017 v2015
- NIST Privacy Framework
- NIST 800-53

- NIST 800-82
- NIST 800-161
- NIST 800-171
- PCIDSS v3.2
- US CMMC 2.0 Level 1
- US CMMC 2.0 Level 2
- US CMMC 2.0 Level 3
- US FEDRAM
- HIPPA HICP
- SOX
- US TX-RAMP Level 1
- US TX-RAMP Level 2
- US TX- Cybersecurity act
- US Privacy Shield
- US FERPA
- WISP Framework

How do I get started with ASCENT Portal?

To get started with the ASCENT Portal you can request a demo on the ASCENT Portal website or reach out to <u>sales@ASCENT-Portal.com</u>. Once you sign up, our support team will work with you to onboard you and your team.

How often is my Portal environment being monitored?

ASCENT Portal provides real-time monitoring, which means your Portal is consistently checking to ensure the controls are in place. Our calendar feature spaces out the work throughout the year to ensure every stakeholder can reasonably keep up with the workload and look ahead to plan their time. If there are controls that are out of date or going to be overdue soon, the Portal will automatically remind stakeholders of the assignment.

Can I edit or change my policies at any time?

Security Compliance Policies can be edited or changed to align with organizational needs, and an annual review is mandatory to ensure their relevance and compliance.

How does ASCENT Portal address the challenge of vendor compliance for organizations?

• Conducting thorough risk assessments to evaluate the security practices of vendors before onboarding.



- Implementing a vendor selection process that includes evaluating the security posture of potential vendors.
- Ensuring that vendor contracts are up to date and stored in a centralized place.
- Conducting periodic audits of vendor practices to verify compliance with contractual security requirements and industry standards.
- Utilizing security questionnaires or assessments to gather information from vendors about their security practices.
- Ensuring that vendors are aware of and comply with relevant regulatory requirements that may impact the organization's overall compliance.

What tools come with ASCENT Portal?

- Security Control Assessments
- Security Compliance Calendar
- Artifact Library
- Dashboards
- Generated Reports
- Vendor Management
- Training Modules
- Business Continuity
- Help Guides

What kind of support or assistance does ASCENT Portal provide in case of security incidents or breaches?

In case of a security incident or breach, you will need to fill out the Incident Response Management form found in the ASCENT Portal. If you are subscribed to ASCENT Portal CISO Services, then email us at <u>Support@ASCENT-Portal.com</u> where you can directly connect with the Security team.



Chapter 2: Getting Started

Getting signed up and logged in for the first time

You will receive an email from support@ASCENT-Portal.com with a link that allows you to join your ASCENT Portal tenant.

Welcome to the ASCENT Security and Compliance Portal! ASCENT is your ONE STOP for Managing Security and Compliance Controls for your organization. Join For added security, this link will only work for 24 hours after it was sent. If you need a new link, request a password reset, follow the Instructions and then sign in here.	Welcome Sheffali Jain
Join For added security, this link will only work for 24 hours after it was sent. If you need a new link, request a password reset, follow the instructions and then sign in here.	Welcome to the ASCENT Security and Compliance Portal! ASCENT is your ONE STOP for Managing Security and Compliance Controls for your organization.
For added security, this link will only work for 24 hours after it was sent. If you need a new link, request a password reset, follow the instructions and then sign in here.	Join
	For added security, this link will only work for 24 hours after it was sent. If you need a new link, request a password reset, follow the instructions and then sign in here.

Click the **join** button, and you will be prompted first to accept the terms and conditions, and then to create a username and password.





VV	elcome
Asc	cent security compliance portal
☑ E Con	By clicking on this checkbox, I agree to the Terms & ditions and the Privacy Policy for the Portal
Plea	se set your new password
â	New Password
â	Confirm Password

Here is a direct link to the Portal: ascentui.com

If you encounter any issues during this process or have questions, feel free to reach out to our support team at <u>Support@ASCENT-Portal.com</u>.

How to reset your password

If you find yourself in need of a password reset for the ASCENT Portal, please follow the steps outlined below:

- 1. Follow this link to the Portal: ascentui.com
- **2.** On the login page, you will first be asked to enter your **Ascent Portal Client Code**, this is the name of your organization.





- **3.** Once you pass this page you will see the login screen that will ask for your **Email and Password**. Click on the **Forgot Password link** seen in the image below.
- 4. Enter the email address associated with your user credentials. If you are unsure about your user credentials, please contact support@ASCENT-Portal.com for assistance.





- 5. An automatic email from ASCENT Portal will be sent to the provided email address.
- 6. In the email, locate and click on the **Reset Button.** This will redirect you to a page where you can set a new username and password.

Cancel

, rd,
click the button below. from now)

How to get support for the Portal

If you need support with functionality of the Portal, logging in, or other Portal-related issues, please log a ticket with our support team.

A ticket can be logged in two ways:

- 1. Email a brief description of the issue to support@ASCENT-Portal.com.
- 2. Log a ticket via the Support page of the Portal.
 - a. Log into the Portal
 - b. Click **About** on the top menu bar (1)
 - c. Click **Support** on the left bar (2)
 - d. Fill in the information, and click **Save** (3)
 - e. This will log a ticket with our support team just like emailing a ticket request. Our support team will reach out to you via the email address you provide.



ASCENT PORTAL	Assessment & Compliance Governance Dusiness Continuity Cybersecurity Vendor Management Training Reports About Admin	Lindsey Tomasko (Whitehat Virtual Technologies)
4 5.0		
E Reference Library	Contact Details	
E ASCENT Release Notes	Name *	
E., News		
Add Additional Users	Emal Address *	
Enhancement Requests	Prone Number	
😧 Support	Sumay* 2	
	Oversity Parks produka skaladi desorption art induk soverenbus when pasable.	
	3	

If a ticket is logged via email, a response will be sent back to confirm that the ticket was logged and provide a ticket number. If you need to check the status of the ticket, you can reply right to that email.

Re: Submitting a New Ticket Example - New Ticket Logged [ID:0002929]
Support <support@ascent-portal.com> To • Lindsey Tomasko</support@ascent-portal.com>
(i) If there are problems with how this message is displayed, click here to view it in a web browser.
CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize th
Thank you for contacting the Service Desk on 12/21/2023 11:26 .
Your ticket has been logged with ID 0002929.
Should you wish to provide any more information that would help us, please reply to this e-mail.
Thank you.
Ascent - Support Ascent Portal



Once the issue has been resolved and the ticket is closed, you will receive a response via email to confirm that the ticket is closed.

On this page, you can vote on the level of satisfaction of our support, which is consistently reviewed by our support team, and greatly appreciated!

Glossary

Artifact - An artifact refers to a document, file, record, or any other evidence that demonstrates the implementation and effectiveness of security controls and measures within an organization. Artifacts are used to provide proof of compliance with specific security standards, policies, or regulatory requirements.

Assessment and Compliance - Identify, schedule, and track important compliance dates. This includes reports, audits, training and operational events. Set due dates and monitor the status of your individual and recurring controls to help ensure regulatory compliance. Re-assign the controls to department specific owners as needed.

Audit Management within a Security Compliance Portal is a systematic approach to planning, executing, and documenting audits. It provides the tools and processes necessary for organizations to maintain a secure and compliant environment while fostering continuous improvement in their security practices.

Business continuity - Business Continuity within a compliance Portal provides a comprehensive framework for disaster preparedness, compliance assurance, and operational resilience. It allows organizations to store and manage critical information in a centralized and accessible manner, facilitating effective response and recovery efforts.

Controls - Controls are fundamental and foundational policies and procedures that need to be established early in any organization. In the ASCENT Portal, a Control is associated with Control ID and Control Description.

Control Description - Description is the brief of the policy or procedure which needs to be implemented in the organization.

Control Families - A Control Family is a set of security controls derived from Frameworks. Each Control is divided into either repetitive or non-repetitive controls. Repetitive controls could be set to repeat annually, semi-annually, quarterly, or monthly.

Control ID - Control ID is the unique number given to each control.

Email Notifications/Reminder's – Receive Automatic Email Reminders when the control has been assigned and completed.

Framework - The framework consists of several documents that clearly define the adopted policies, procedures, and processes by which the organization abides. It effectively explains to all parties (internal, tangential, and external) how information, systems and services are managed within your organization. The main point of having an information security framework in place is to reduce risk and exposure of the organization due to vulnerabilities.



The framework is your go-to document in an emergency. For example, if someone breaks into your system, it outlines daily procedures that are designed to reduce risk. Implementing information security frameworks provides advantages by instilling confidence or establishing a strong reputation with potential business partners and customers. The frameworks allow the agents to understand how you will protect their data from harm.

Some examples of Frameworks are ISO 27001, PCI Standards, COBIT, HITRUST, TSP2017 and so on. Each Framework consists of Control Families and the Controls required by the organization to be Compliant.

Governance - Store all your policies, whitepapers and plans in a centralized place and access the documents anytime you need them. Extract the governance report to quickly and easily share with Stakeholders.

Overdue tasks/My Overdue Tasks - Quick snapshot of the pending tasks which need to be completed by the organization, or specifically by you.

Policy Management Store - User can maintain a living set of policies that is easily accessible.

Tenant - A tenant refers to an entity or organization that utilizes the Portal to manage and address its security compliance requirements specific to its operations. Each tenant operates within its own segregated space or instance within the Portal, ensuring that their data, configurations, and compliance records are distinct and separate from other tenants.

This concept of multi-tenancy allows the security compliance Portal to serve multiple organizations or clients efficiently, providing them with a shared platform while maintaining data isolation and security. It enables each tenant to customize and manage its security policies, compliance frameworks, and user access within the Portal to align with its unique needs and regulatory environment.

Vendor Management - With the increased use of vendors comes the need for increased oversight. You can avoid complicated spreadsheets, manually updating calendars, and trying to organize files across network folders. Store your files, documents, and contracts in one place.

Dashboard

Below we will review the purpose of the dashboard and how to utilize it.

Purpose of the user dashboard

The dashboard is an excellent way to quickly see the current state of your security posture within the Portal, and know what areas need attention.

The dashboard is also a great way to show the current state to executive leadership or other stakeholders that don't often work within the Portal but need an update on the status of the organization's security posture.

To navigate to the user dashboard:

- 1. Click Assessment & Compliance (1)
- 2. Click Dashboard (2)
- 3. Choose the framework you would like to see from the dropdown menu (3)



Using the user dashboard

These features collectively provide a holistic view of the compliance landscape, offering both high-level insights and detailed information for effective management and decision-making. Whether you need a quick overview or a deep dive into specific control families, the Security Compliance Portal is designed to cater to your diverse needs.

Current Compliance Score (4) - Use the Current Compliance Score to get an instant overview. Green indicates areas in compliance, yellow signals attention needed soon, and red flags areas out of compliance requiring immediate attention.

Monthly Score Trend (5) - this feature allows you to track trends across your organization throughout the year. This is a valuable tool for planning assignments, staffing schedules, and more.

Control Status Graph (6) - illustrates the number of controls in each status: in place, not in place, or not applicable. This gives you a quick snapshot of your organization's control status distribution.

Control Family Score (7) - provides an overview of all control families. Quickly spot which families need attention based on the assigned criticality. This feature allows you to prioritize efforts effectively.

The list of Control Families (8) - Navigate through the list of Control Families to see individual scores. This feature enables you to quickly assess the score for each family and delve into specific details for a more comprehensive understanding.



Notifications and Alerts to Help Manage Controls



Purpose of notifications and alerts

The automated notifications and alerts help each stakeholder keep track of their upcoming assignments, without the extra lift of a project manager to schedule the tasks.

If the owner of a control changes, the notifications automatically update to the new owner, so the admin does not need to manually update this.

An automated email will be sent to the assigned control owner:

- 1. When a control has been assigned to them.
- 2. When a control is 5 days from being due.
- 3. When a control is 3 days from being due.
- 4. When a control is completed.
- 5. When a control is reassigned to a new control owner.

Note: Automated alerts cannot be modified.

Calendar

Purpose of the calendar

The Security Compliance Calendar serves as a centralized tool within a security compliance Portal to facilitate the management of controls and compliance-related tasks throughout the year.

Navigating to the calendar

- 1. Click Assessment & Compliance (1):
- 2. Click Security & Compliance Calendar (2):
- 3. Choose the framework from the dropdown menu (3):
- 4. View the Calendar:
 - a. After selecting the framework, choose the desired view mode for the calendar. Options include: (4)
 - i. Day View: Display events and tasks for a specific day.
 - ii. Week View: Show a weekly overview of security and compliance activities.
 - iii. **Month View:** Provide a monthly calendar highlighting key events and due dates.
- 5. Legend of what each color means: (5)
 - a. Green = controls are complete, and everything is in compliance
 - b. Yellow = due date for a control is coming up soon
 - c. Red = a control is overdue and needs attention immediately



ASCENT PORTAL	Assessment & C	omplia	nce Governance Bu	siness Continuity Vendo	or Management Training	Reports About Ad	min		Jason Phillip (Curio F	Publishi
Admin Dashboard	HIPAA/HITRUST.	Level		1						
Dashboard	Month Week	Day			January 2024	L		Coday	Control Family	#
Security Control				1					0.0. Information Security Management Program	n 6
ssessment	Sun		Mon	Tue	Wed	Thu	Fri	Sat	1.0. Access Control	129
curity & Compliance	<u> </u>	31	1 448: Acceptance criteria	2 451: Protection against m	3 464: If a network-based	4 457: The checks carried (5 460: Bring your own devi	6	2.0. Human Resources Security	58
			449: Managers ensure th	452: Formal policy contro	455: Anti-malware softw	458: Formal policy contri	461: Mobile code must be		3.0. Risk Management	16
Compliance Controls			450: Detection, preventic	453: Periodic reviews/sco	456: Procedures are defi	459: Antimalware user a	462: Automated controls		4.0. Security Policies	7
ntrols Assigned to Me		7	8	9	10		1 2	13	5.0. Organization of Information Security	99
			463: Policy controls are it 464: Back-up copies of it	466: Complete restoration 467: Back-ups are stored	469: When the back-up 470: Roles and responsib	472: Network managers i 473: When configuring w			6.0. Compliance	36
lfact Library			465: A formal definition c	468: Regular testing of b	471: Networks are manaç	474: A current network d			7.0. Asset Management	18
		14	15	16	17	18	19	. 20	8.0. Physical Security and Environmental Security	62
			175: Network architectur 176: All authorized and u	478: The ability of the net 479: Formal procedures I	481: The use of removabl 482: Media containing co	484: Procedures for hand 485: Administrator docu	487: Attempts to obtain I 488: System documenta		9.0. Communications and Operations	126
			477: Security features, se	480: Controls (e.g., polici	483: Media is disposed o	486: User documentation	489: Formai exchange pr		Management	
		21	22	23	24	25	26	27	10.0. Information Systems Acquisition, Development and Maintenance	55
			490: Communications pr	493: Retention and dispa	496: Personnel are appro	499: Personnel are appro	502: Agreements are est		11.0. Information Security Incident Management	1 21
			491: Anti-maiware solutk 492: Personnel responsit	494: Controls and restric 495: Terms and condition	497: Personnel are appro 498: Personnel are appro	500: Personnel are appro 501: Personnel are appro	503: Exchange agreemer 504: Exchange agreemer		12.0. Rusiness Continuity Management	42
		_								42
		28	29	30	31	E12 Deliales encoderate	2		13.0. Privacy Practices	00
			506: Exchange agreeme	508: Exchange agreemer	511: Exchange agreemen	514: Media containing in	518: Processes and techr			
				509: Exchange garacime	512: Exchange agreemen	515: Procedures are esta	519: Legal considerations			

Artifacts

What is an artifact and what is its purpose?

An artifact refers to a document, file, record, or any other evidence that demonstrates the implementation and effectiveness of security controls and measures within an organization. Artifacts are used to provide proof of compliance with specific security standards, policies, or regulatory requirements.

How to upload artifacts

- 1. Click on Assessment & Compliance (1).
- 2. Click on Security Control Assessment (2).
- 3. Click the desired Control Family Name (3).
- 4. Check the appropriate status of the control (4).
- 5. Click Upload Artifacts (5).
- 6. Click the **blue upload button (6).** Choose the file you want to upload from your saved folders and double-click on it to upload it.
- 7. The newly added document will appear in the list (7). Click the **X** to close the pop-up box.
- 8. You'll now see a number next to Upload Artifacts, which confirms how many documents are saved to that control (8).
- 9. Click Submit (9).



	WISP Framework						
board	K						
	Control Family Name	Score	Answered/Total	In Place	Not In Place	Not Applicable	Last Updat
rol	Cybersecurity & Dacy Governance	0%	0/1 - 00%	0	0	0	12/26/2023
	2. Asset Management	0%	0/1-00%	0	0	0	12/26/202
mpliance	3. Cloud Security	0%	0/1 - 00%	0	0	0	12/26/202
	4. Configuration Management	0%	0/2 - 00%	0	0	0	12/26/202
e Controis	5. Continuous Monitoring	0%	0/3 - 00%	0	0	0	12/26/202
gned to Me	6. Cryptographic Protections	0%	0/5 - 00%	0	0	0	12/26/202
nce	7. Data Classification & Handling	0%	0/3 - 00%	0	0	0	12/26/202
CEDS)	8. Endpoint Security	0%	0/9 - 00%	0	0	0	12/26/202
γ	9. Identification & Authentication	0%	0/11 - 00%	0	0	0	12/26/2023
	10. Mobile Device Management	0%	0/1-00%	0	0	0	12/26/2023
	11. Network Security	0%	0/3 - 00%	0	0	0	12/26/2023
	12. Privacy	0%	0/2 - 00%	0	0	0	12/26/2023
	13. Security Awareness & Training	0%	0/13 - 00%	0	0	0	12/26/2023
	14. Technology Development & Acquisition	0%	0/1 - 00%	0	0	0	12/26/2023
	15. Vulnerability & Patch Management	0%	0/2 - 00%	0	0	0	12/26/2023
	16. Web Security	0%	0/1 - 00%	0	0	0	12/26/2023
	IZ. Change Management Assessment & Compliance Governance Business Continuity. Othersee	Uni	0/2 - 00%		Items pe	ərpage: 50 ⊽ 1 ·	- 17 of 17
DRTAL)	Change Management Assessment & Compliance Governance Business Continuity Cybersec	urity Vendor Management Reports Abor	u/2 - 00%		items pe	er page: 50 + 1 ·	- 17 of 17 Toe Duje (GILL C
DRTAL)	I.Z. Change Management Assessment & Compliance Governance Business Continuity Cybersec Back to Ouestionnaire	urity Vendor Management Reports Abor	0/2 - 00%. At Admin		i Items pe	ər page: 50 - 1 -	- 17 of 17 Toe Duje (GILL C
DETAL)	12. Chonge Management E Assessment & Compliance Governance Back to Ouestionnaire	urity Vendor Management Reports Abor	0/2 - 00%. .t Admin		i items pe	or page: 50 √ 1 ·	- 17 of 17 Toe Duje (GILL C
ind		urity Vendor Management Reports Abor	0/2 - 00%. It Admin		i items pe	ar page: 50 √ 1 ·	- 17 of 17 Toe Duje (GILL C
DRTAL)	I. Change Management Assessment & Compliance Governance Business Continuity Cybersec Back to Questionnaire I. Cybersecurity & Privacy Governance GOV-07 Mechanisms exist to establish contact with selected gro - facilitate angoing cybersecurity and privacy education and to - socialitate angoing cybersecurity and privacy education and to - socialitate angoing cybersecurity and privacy education and to - socialitate angoing with recommended cybersecurity and privacy	urity Vendor Management Reports Abor urity Vendor Management Reports Abor ups and associations within the cyberse ining for organizational personnel: y practices, techniques and technologie burdbillike each incidence	u/2 - 00%. It Admin curity & privacy communit s; and	es to:	i Rems po	er page: 50♥ 1 ·	Toe Duje (GILL C
DRYAL) a loard of mpliance e Controls	I. Change Management Assessment & Compliance Governance Business Continuity Cybersec Back to Ouestionnaire I. Cybersecurity & Privacy Governance GOV-07 Mechanisms exist to establish contact with selected gro - Facilitate angoing cybersecurity and privacy education and tra - Maintain currency with recommended cybersecurity and privacy - Panding Auditor Approval	urity Vendor Management Reports Abor ups and associations within the cyberse ining for organizational personnel; y practices, techniques and technologie Interabilities and incidents.	u/2 - 00%. At Admin curity & privacy communit s; and	es to:	Rems po	er page: 50 v 1 ·	- 17 of 17 Toe Duje (GILL C
orran or		unity Vendor Management Reports Abor unity Vendor Management Reports Abor ups and associations within the cyberse ining for organizational personnel: ry practices, techniques and technologie inerabilities and incidents.	u/2 - 00%. At Admin curity & privacy communit s; and	es to:	Rems po	ar page: 50 1 ·	17 of 17
In the second se	I. Change Management Assessment & Compliance Governance Business Continuity Cybersec Back to Ouestionnaire I. Cybersecurity & Privacy Governance GOV-07 Mechanisms exist to establish contact with selected gro - Cacillate angoing cybersecurity and privacy education and the Naintain currancy with recommended cybersecurity and privacy - Control in Place Control In Place Control Not in Place Control Not applicable Control Not in Place Control Not Plac	urity Vender Management Reports Abor ups and associations within the cyberse ining for organizational personnel; ry practices, techniques and technologie inerabilities and incidents.	0/2 - 00%. It Admin curity & privacy communit	es to:	C Rems po	ar page: 50 √ 1 ·	Toe Duje (GILL C
orral oorral of e Controls (controls (controls (controls))	I. Crhange Management Assessment & Compliance Governance Business Continuity Cybersec Back to Ouestionnaire I. Cybersecurity & Privacy Governance GOV-07 Mechanisms exist to establish contact with selected gro - Facilitate angoing cybersecurity and privacy education and the Maintain currency with recommended cybersecurity and privacy - Sonitate angoing cybersecurity and privacy education and the Maintain currency with recommended cybersecurity and privacy - Control In Place - Control In Place - Control In Place - Control In Place - Control Answer (if applicable) - Control Answer (if applicable) - Control Maxwer (if	urity Vendor Management Reports Abor ups and associations within the cyberse ining for organizational personnel: y proctices, techniques and technologie inerabilities and incidents.	0/2 - 00%. At Admin curity & privacy communit Is; and	es to:	i Rems po	er page: 50 1 ·	Toe Duje (GILL C
orral oard of e Controls ped to Me occ	I. Chonge Management Assessment & Compliance Governance Business Continuity Cybereed Back to Ouestionnaire I. Cybersecurity & Privacy Governance OOV-07 Mechanisms exist to establish contact with selected gro - Facilitate angoing cybersecurity and privacy education and that Maintain currency with recommended cybersecuting and privace - Share current security-related information including threats, vu Pending Alador Approval Ocontrol in Place Not Applicable Control Answer (if applicable) Sident Updead Antfacts (0) Note Assign	urity Vendor Management Reports Abor ups and associations within the cyberse ining for organizational personnel. y practice, techniques and technologie inerabilities and incidents.	0/2 - 00%. At Admin curity & privacy communit Is; and	és to:	i Rems po	er page: 50 → 1 ·	- 17 of 17 Toe Duje (GILL C
oorration of mplance e Controls (mplance trans) (mplance e Controls (mplance e Control	I. Change Management Assessment & Compliance Governance Business Continuity Cybersec Back to Questionnaire OOV-07 Mechanisms exist to establish contact with selected gro Control to ngoing cybersecurity and privacy education and the Naintian currency with recommended cybersecurity and privacy Control in Place Control In Place Control Answer (if applicable) Stehnik Uyboad Artifacts (0) Notes Ausign Back to Questionnaire	urity Vendor Management Reports Abor ups and associations within the cyberse ining for organizational personnel: y procetices, techniques and technologie inerabilities and incidents.	0/2 - 00%. At Admin curity & privacy communit is; and	es to:	i Rems po	er page: 50 → 1 ·	Toe Duje (GILL C
orral) noard mpilance e Controls pred to Me scoe	I. Change Management Assessment & Compliance Governance Business Continuity Cybersec Back to Ouestionnaire I. Cybersecurity & Privacy Governance OOV-07 Mechanisms exist to establish contact with selected gro coalitate angoing cybersecurity and privacy education and the coalitate angoing cybersecurity and privacy coation in Place Coatrol In Place Control In Place Control In Place Control In Starse (I opplicable) Setent Upload Autfacts (0) Note Assign Back to Questionnaire	urity Vendor Management Reports Abor ups and associations within the cyberse ups and associations within the cyberse practices, techniques and technologic inerabilities and incidents.	d)/2 - 00%. A Admin curity & privacy communit s; and	es to:	Rems po	ar page: 50 - 1 -	Toe Duje (GILL C
oord oord mpilonce e Controls ince into; ince into;	I. Change Management Assessment & Compliance Governance Business Continuity Cybersec Back to Questionnaire OV-07 Mechanisms exist to establish contact with selected gro - Collitate ongoing cybersecurity and privacy education and tar - Naintain currency with recommended cybersecurity and privacy - Control In Place O Control In Place O Control In Place O Control In Place O Control Answer (if opplicable) Steme Upboad Antifacts (i) Rete Ausign Back to Questionnaire	urity Vender Management Reports Abor ups and associations within the cyberse ining for organizational personnel; y procetices, techniques and technologie inerabilities and incidents.	t Admin curity & privacy communit is; and	es tα:	C Rems po	ar page: 50 → 1 -	Toe Duje (GILL C



ASCENT PORTAD	=	Assessment & Compliance	Governanc	e Business Continu	uity Cybersec	urity Vendor Ma	nagement Reports	About Admin					Toe Duje (GILL Co	rp) 🔒
Auditor Dashboard		Back to Ouestionnaire												
Dashboard Security Control Assessment		1. Cybersecurity & Privac	y Govern	ance										
Security & Compliance Calendar		GOV-07 Mechanisms exi • Facilitate ongoing cybe • Maintain currency with	at to esta rsecurity recomme	iblish contact with and privacy educ ended cybersecuri	selected gro ation and tra ity and privac	ups and associa ining for organiz cy practices, tecl	ations within the cyb rational personnel; hniques and techno	ersecurity & privacy co logies; and		ities to:				
E All Compliance Controls		Share current security Pending Auditor Approv	Upload	d Artifacts								×		
₽, Controls Assigned to Me		Control in Place Control Not in Place	Filter			Ŷ	ł		6	_	> (
Control Evidence Documents (CEDs)		O Not Applicable Control Answer (if appli		/										
III Artifact Library		-		Name		Created By		Created On	Size ((Kb) Action				
		Submit Upload A						Items per page:	10-	0 of 0				
		Back to Questionnaire												
0														

security	Upload A	rtifacts				;	×
	Filter		Ψ			0	
e (if appli	↑ /						
		Name	Created By	Created On	Size (Kb)	Action	
		Ascent logo.png	Toe Duje	12/26/2023	n		
Upload A				Items per page:	10-1-1	of 1 < >	



ASCENT PORTAL	Assessment & Compliance Governance Business Continuity Cybersecurity Vendor Management Reports About Admin	Toe Duje (GILL Corp)
Auditor Dashboard	Back to Questionnaire	
🕂 Dashboard	Construction of the second sec	
Security Control Assessment	1. Cybersecurity & Privacy Governance	
Calendar	GOV-07 Mechanisms exist to establish contact with selected groups and associations within the cybersecurity & privacy communities to: • Facilitate ongoing cybersecurity and privacy aducation and training for arganizational personnel; • Maintian currency with recommended cybersecurity and privacy practices, techniques and technologies; and	
E All Compliance Controls	Share current security-related information including threats, vulnerabilities and incidents. Pending Auditor Approval	
■, Controls Assigned to Me	O Control in Place O Control Not in Place	
Control Evidence Documents (CEDs)	O Not Applicable Control Answer (if applicable)	
artifact Library		
	Submit Uplead Artifacts (1) Notes Assign	
9	Back to Questionnaire 8	
0		

How to delete artifacts

- 1. Click **Upload Artifacts (1)**.
- 2. **Check the box** next to the artifact you want to delete (2).
- 3. Click the **X** (3).
- 4. Click **OK** in the pop-up menu (4).

00 Internal and external issues that are relevant to the purpose or mission of the organization, along with the ability to achieve the intended outcomes of the Security Program have been identified and documented. [ISO 27001 Control Reference: Clause 4.1]
O Control in Place
Control Not In Place
O Not Applicable
Control Answer (if applicable)
Please refer to the Security Program Planning Policy.
Submit Upload Artifauts (1) Notes Assign (Bryon Miller - Whitehall)



Assessment & Compliance Governance Business Contin	uity Cybersecurity Vendor	login.ascent-portal.com says	files?				Lindsey Tomasko (Whitehat Virtual Technol
Back to Questionnaire		Are you sure you wont to delete the selected	ок	Cancel			
01. SECURITY PROGRAM PLANNING							
001 Internal and external issues that are relevant to Pending Auditor Approval O Control in Place © Control Not in Place	the purpose or mission of	the organization, along with the ability to achiev	e the intended ou	itcomes of t	he Security I	Program	n have been identified and documented. [ISO 27001 Control Reference: Clause 4.1]
O Not Applicable Control Answer (if applicable)	Upload Artifacts	_					×
Please refer to the Security Program Planning Policy Submit Upload Arstacts (1) Notes	Filter	¥				٥	◎ ≪ 3
002 External entities that have an interest in the	Name	Created By	Created On	Size (Kb) Act	ion	e: Clause 4.2]
O Control in Place	Ascent logo.	Lindsey Tomasko	12/21/2023		11 [2		
Control Not in Place Not Applicable Control Answer (if applicable)	-		Items per page:	10•	1 – 1 of 1	<	
Please refer to the Security Program Planning Policy.		' 2					
Submit Upload Artifacts (0) Notes	Assign (Bryon Miller - Whitehat)	-					
003 The scope of the Security Program is based on security controls have been determined to define th Pending Auditor Approval	external issues, internal iss he scope of the Security Pr	ues, requirements of interested parties, and rela gram. The scope of the Security Program has b	itionships betwee een documented	n activities p and made o	performed b available to	y the org all appro	rganization and those performed by other organizations. The boundary and applicable ropriate personnel. [ISO 27001 Control Reference: Clouse 4.3]

Viewing and downloading all artifacts

- 1. Click Assessment & Compliance (1)
- 2. Click Artifact Library (2)
- 3. Here you will see a list of all control families that have an artifact uploaded to them (3).
- 4. The number indicates how many artifacts are in each family (4).
- 5. To download all artifacts into a PDF report or ZIP file, **click the respective button** (5 and 6).

ASCENT PORTAL	Assessment & Compliance Governance	Business Continuity Cyl	persecurity Vendor Manage	ment Reports About Admin			Toe Duje (GILL Corp)
🕂 Auditor Dashboard	WISP Framework	1					•
🕂 Dashboard	Download All Artifacts (ZIP) Download Arti	ifacts List (PDF)	6				
Security Control Assessment							
Calendar	Filler Control Family Name / Task Name	5 ontrol ID	Control Status	Comment		Last Updated	Artifacts Uploaded
E All Compliance Controls	Cybersecurity & Privacy Governance	GOV-07				12/26/2023	1
■ Controls Assigned to Me	N				ltems pe	page: 15 *	1-1of1 < >
Control Evidence Documents (CEDs) C23 Artifact Ubrary	← 0	3					4
0							



Reports

Automated Weekly Status Reports

Status Reports provide a real-time status of every control contained in the selected control framework. Status Reports are automatically generated by ASCENT Portal every week and stored in the Reports tab.

These reports contain the following graphical representations:

- 1. Overall Risk Score
- 2. Control Status
- 3. Control Family Scores
- 4. A list of all overdue controls and the assigned control owner for each

How to find the automatically generated reports

- 1. Click Reports (1)
- 2. Click Status Reports (2)
- 3. Here you will see the Scheduled Reports folder, which is where the auto-generated reports will be kept. (3)
- 4. Click the folder's name to see a list of all the reports in that folder (4).





tive Action Plans						-
	Filter	Ŷ				C
	^	Scheduled Reports				
		Name	Created By	Created On	Size (Kb)	Action
		WeeklyReport_2022 SOC 2 Assessment_20220508.pdf	Portol Admin	05/08/2022	382	
		WeeklyReport_2022 SOC 2 Assessment_20220515.pdf	Portal Admin	05/15/2022	379	
		WeeklyReport_2022 SOC 2 Assessment_20220522 pdf	Portal Admin	05/22/2022	376	
		WeeklyReport_2022 SOC 2 Assessment_20220529.pdf	Portal Admin	05/29/2022	368	
		WeeklyReport_2022 SOC 2 Assessment_20220605.pdf	Portol Admin	06/05/2022	360	
		WeeklyReport_2022 SOC 2 Assessment_20220612.pdf	Portal Admin	06/12/2022	357	
		WeeklyReport_2022 SOC 2 Assessment_20220619.pdf	Portol Admin	06/19/2022	349	
		WeeklyReport_2022 SOC 2 Assessment_20220526.pdf	Portal Admin	06/26/2022	338	
		WeeklyReport_2022 SOC 2 Assessment_20220703.pdf	Portal Admin	07/03/2022	338	
		WeekbyReport_2022 SOC 2 Assessment_20220710.pdf	Portal Admin	07/10/2022	330	
				Items per page: 1	0₩ 1 - 10 of 2	99 <

Generating framework reports manually

- 1. Click Reports (1)
- 2. Click Security Assessment Reports (2)
- 3. Click the **framework** from the dropdown menu that you need a report on (3)
- 4. Click Generate Report (4)
- 5. Once the report is generated, it will appear in your 'downloads' folder on your computer, and you are provided the ability to modify the filename of the report and save it.
 - a. Click the **folder icon** (5) to create a new folder, and name it something fitting.
 - b. Once in that folder, click the **upload icon** (6) to add the newly generated report to that folder.
 - c. It is recommended that all reports be uploaded to ASCENT Portal for centralized storage and safekeeping.
- 6. Here you will see the folder name you just created. When you click the name, you'll find the report you uploaded to said folder (7).



ASCENT PORTAL	Assessment & Compliance Governance	Business Continuity Cybersecurity Ve	ndor Management Reports About Admin		Toe Duje (GILL Corp)
Security Assessment Reports	WISP Framework				56
Status Reports	Generate Report		0		
2 WISP	Filter	Ŷ			00
	↑ /				
	Name Name		Created By	Created On	Size (Kb) Action
	WISP Reports		Toe Duje	12/26/2023	
	1			Items per page:	10▼ 1 – 1 of 1 < >
	7				
0					



Chapter 3: Using the Portal General Portal

Types of Access

Below are the types of access and what each type has access to.

Modules	Sections	MSP	Tenant Admin	Tenant Users
Assessment & Compliance	MSP Dashboard	Х		
Assessment & Compliance	Admin Dashboard		Х	
Assessment & Compliance	Dashboard	Х	X	Х
Assessment & Compliance	Security Control Assessment	Х	X	Х
Assessment & Compliance	Security Compliance Calendar	Х	X	X
Assessment & Compliance	All Compliance Controls	Х	X	X
Assessment & Compliance	Controls Assigned to me	Х	X	Х
Assessment & Compliance	Artifact Library	Х	X	Х
Governance	Policies	Х	X	Х
Governance	Policies and Templated	Х	X	X
Governance	Incident Response	Х	X	Х
Business Continuity	BC Strategic Plan	Х	X	Х
Business Continuity	BC/DR Plans	Х	X	Х
Business Continuity	Call Trees	Х	X	Х
Business Continuity	Test Scripts	Х	X	Х
Business Continuity	Test Reports	Х	X	Х
Business Continuity	Event Reports	Х	X	X
Vendor Management	Vendor List	Х	X	X
Vendor Management	Vendor Reports	Х	X	Х
Vendor Management	Vendor Contacts	Х	X	Х
Vendor Management	Manage Contracts	Х	X	Х
Reports	Security Assessment Report	Х	X	Х
Reports	Status Report	Х	X	Х
Reports	WISP Report	Х	X	X
Admin	Reference Library	Х	X	X
Admin	Ascent Release Notes	Х	X	X
Admin	News	Х	X	Х
Admin	Enhacement Request	Х	X	Х
Admin	Manage Tenant	Х	X	



Adding New Users to the Portal

- 1. Click **Admin** (1)
- 2. Click Managed Tenant User (2)
- 3. Click the **plus sign** to add a new user (3)
- 4. Fill in the missing information of the new user (4)
- 5. Once complete, click **Submit** (5)
- 6. Here you will see the list of all user accounts (6)
- 7. Click **Edit** should you need to edit the user's information or access (7)

	3		_	-	¥	Filter
Action	Status	Created On	User Type	Email	Name	User ID
Edit	Active	12/26/2023	MSP Admin	ann.marryl@ttcorp.com	Ann Marryl	675
Edit	Active	12/26/2023	Tenant Admin	Toe.duje@Gill.com	Toe Duje	676
Edit	Active	12/26/2023	Tenant User	tom.cher@gill.com	Tom Cher	677
Edit	Active	05/07/2020	Tenant Admin	sheffali.jain@whitehatvirtual.com	Whitehat Virtual admin	12
1-4 of 4 < >	ems per page: 15 ~	Ite				

ASCENT PORTAL	Assessment &	& Compliance Governance B	usiness Continuity Cybersec	urity Vendor Management Reports Abo	ut Admin			Toe Duje (GILL Corp) 🔒
Amanage Tenant User	Filter		¥					• •
	User ID	Name	Ema	a	User Type	Created On	Status	Action
	675	Ann Marryl	ann	.marryl@ttcorp.com	MSP Admin	12/26/2023	Active	Edit
	676	Toe Duje	Add New Tenant Liser	1	**********	12/26/2023	Active	Edit
	677	Tom Cher	Add Hell Tendin Oser			12/26/2023	Active	Edit
		Whitehat Virtual adm	First Name			05/07/2020	Active	Edi
			Last Name				Items per page: 15 +	1 - 4 of 4
			Email					
			Time Zone	Central Standard Time		•		
			Status	Active		•		
			User Type			•		
			Access Type			· • ·		
					5 Sub	mit		



ASCENT PORTAL	Assessment & C	compliance Governance Business Continuity	Cybersecurity Vendor Management Reports About Adm	in			Toe Duje (GILL Corp)
Manage Tenant User	Filter	6					• •
	User ID	Name	Email	User Type	Created On	Status	Action
	675	Ann Marryl	ann.marryl@ttcorp.com	MSP Admin	12/26/2023	Active	Edit
	676	Toe Duje	Toe.duje@Gill.com	Tenant Admin	12/26/2023	Active	Edit
	677	Tom Cher	tom.cher@gill.com	Tenant User	12/26/2023	Active	Edit
	12	Whitehat Virtual admin	sheffali.jain@whitehatvirtual.com	Tenant Admin	05/07/2020	Active	Edit
					Ite	ms per 7 e: 15•	1 – 4 of 4 < >

Assigning and Managing Controls

All controls must be assigned to an owner and be given a due date. The owner is responsible for ensuring the control is kept in compliance and will be made automatically via email once the control is assigned to them.

To assign a control:

- 1. Click Assessment & Compliance (1)
- 2. Click Security Control Assessment (2)
- 3. Click on the desired Framework via the drop-down menu (3)
- 4. Click on the desired Control Family Name (4)
- **5.** In the desired control, click **Assign** (5)
- 6. In the popup box, click the **plus sign** (6)
- 7. Click the **User** dropdown, select the appropriate user's name (7)
- 8. Select the appropriate due date for the control (8)
- 9. Type a description if desired (9)
- 10. Check the box if you'd like to create a ticket in your PSA associated with the control assignment (10)
- **11.** Click **Submit** (11)
- 12. You will now see the user's name next to 'Assign' (12)



in ousinoond	K						
board	Control Family Name	Score	Answered/Total	In Place	Not In Place	Not Applicable	Last Update
rity Control	1. Cybersecurity & Privacy Governance	0%	0/1-00%	0	0	0	12/26/2023
amone	2. Asset Management	0%	0/1-00%	0	0	0	12/26/2023
ity & Compliance Idar	3. Cloud Security	0%	0/1-00%	0	0	0	12/26/2023
moliques Controle	4. Configuration Management	0%	0/2 - 00%	0	0	0	12/26/2023
inpitulice controls	5. Continuous Monitoring	0%	0/3 - 00%	0	0	0	12/26/2023
ols Assigned to Me	6. Cryptographic Protections	0%	0/5 - 00%	0	0	0	12/26/2023
ntrol Evidence suments (CEDs)	7. Data Classification & Handling	0%	0/3 - 00%	0	0	0	12/26/2023
	8. Endpoint Security	0%	0/9 - 00%	0	0	0	12/26/2023
t Library	9. Identification & Authentication	0%	0/11 - 00%	0	0	0	12/26/2023
	10. Mobile Device Management	0%	0/1 - 00%	0	0	0	12/26/2023
	II. Network Security	0%	0/3 - 00%	0	0	0	12/26/2023
	12. Privacy	0%	0/2 - 00%	0	0	0	12/26/2023
	13. Security Awareness & Training	0%	0/13 - 00%	0	0	0	12/26/2023
	14. Technology Development & Acquisition	0%	0/1-00%	0	0	0	12/26/2023
	15. Vulnerability & Patch Management	0%	0/2 - 00%	0	0	0	12/26/2023
	16. Web Security	0%	0/1 - 00%	0	0	0	12/26/2023
	17. Change Management	0%	0/2 - 00%	0	0	0	12/26/2023
					linese e		17 of 17

ASCENT PORTAL	Assessment & Compliance Governance Business Continuity Cybersecurity Vendor Management Reports About Admin	Toe Duje (GILL Corp)
🕂 Admin Dashboard	Rack to Questionnaire	
Dashboard		
Security Control Assessment	I. Cybersscunty & Privacy Governance	
Calendar	GOV-07 Mechanisms exist to establish contact with selected groups and associations within the cybersecurity & privacy communities to: • Facilitate ongoing cybersecurity and privacy education and training for organizational personnel; • Maintain currency with recommended cybersecurity and privacy practices, techniques and technologies; and	
E All Compliance Controls	Share current security-related information including threats, vulnerabilities and incidents. Pending Auditor Approval	
⇒ Controls Assigned to Me	O Control in Place O Control Not in Place 5	
Octore Evidence Documents (CEDs)	O Not Applicable Control Answer (if applicable)	
C2 Artifact Library	Submit Upload Antfacts (1) Notes Assign	
	Back to Questionnaire	



ASCENT PORTAD	₽ Ass	sessment & Compliance C	iovernance Busine	ss Continuity Cybersecurity Vend	or Management Reports	About Admin						Toe Duje (GILL Corp) 🔒
Admin Dashboard	Ba	ick to Questionnaire										
E Dashboard												
		Cybersecurity & Privacy	Governance									
Assessment												
Security & Compliance Calendar	GC • Fe	0V-07 Mechanisms exis acilitate ongoing cyber	07 Mechanisms exist to establish contact with selected groups and associations within the cybersecurity & privacy communities to: Eate angoing cybersecurity and privacy education and training for organizational personnel:									
	si Po	Adhibit currency with recommended cybeneounly and privacy practices, techniques and technologies; and hara current security-related information including threats, vulnerabilities and incidents.										
		Control in Place	Assign Task						×			
EV Controls Assigned to Me		Control Not in Place										
Control Evidence		Not Applicable	Filter		Ÿ		6	~	•			
		ontrol Answer (il appli	Date	liner	DSA Ticket		ction	Befreeh				
EE Artifact Library			Date	Use	ron liver	~	CUOII	Refreat				
						Items per page:	15-	0 of 0 <	>			
		Submit Upload A							_			
	Ba	ick to Questionnaire										



ASCENT PORTAL	Assessment & Compliance Governance Business Continuity Cybersecurity Vendor Management Reports About Admin	Toe Duje (GILL Corp) 🔒											
🕂 Admin Dashboard	Back to Questionnaire												
- Dashboard	1 Cuberseruitu & Privacy Governance												
Security Control Assessment		_											
Calendar	GOV-07 Mechanisms exist to establish contact with selected groups and associations within the cybersecurity \$ privacy communities to: • Facilitate angoing cybersecurity and privacy education and training for organizational personnel; • Maintain currency with recommended cybersecurity and privacy practices, techniques and thechnologies; and												
E All Compliance Controls	Share current security-related information including threats, vulnerabilities and incidents. Pending Auditor Approval	rent security-related information including threats, vulnerabilities and incidents. uditor Approval											
E. Controls Assigned to Me	O Control in Place O Control Not in Place												
Control Evidence Documents (CEDs)	O Not Applicable 12 Control Answer (if applicable)												
Artifact Library													
	Submit Upload Artifacts (1) Notes Assign (Toe Duje)												
	Back to Questionnaire												



Managing controls for the organization:

- 1. Click Assessment & Compliance (1)
- 2. Click **All Compliance Controls** (2)
- 3. Choose the desired framework (3)
 - a. You will see:
 - i. How many total controls are in place (4)
 - ii. How many total controls are not in place (5)
 - iii. How many total controls are overdue (6)
 - iv. How many controls will be due soon (7)
 - v. You can filter to see specific control statuses (8) (9)
 - 1. All overdue controls
 - 2. Controls due in 3 days
 - 3. Controls due in 5 days
 - 4. All tasks
 - vi. The control family name (10), assigned owner (11), and due date (12) will be shown in the list.
 - vii. To reassign the owner, change the due date, change the status, or upload an artifact, click **Edit** (13).

ASCENT PORTAL	Assessment & Compl	iance Governance	Business Continui	ty Cybersecurity Vendor Management	Reports About	Admin			Toe Du	uje (GILL Corp) 🔒
	Security Control Fram	ework								
🕂 Admin Dashboard	WISP Framework	-3								•
H Dashboard	Control in Place			Control Not in Place		Overdue Control Tasks		Upcoming Co	ontrol Tasks 👩	
Assessment	0		-	61	-	0	_	(2023)		_
Calendar		us Castrala								
E, All Compliance Controls	Due In 5 Days	9						11	12	13 -
➡, Controls Assigned to Me	Filter 8		Ψ							
Control Evidence Documents (CEDs)	Control Family Name	Control ID	Control Des	cription			C	ontrol Owner	Due Date	Action
🖼 Artifact Library	Cybersecurity & Privacy Governance	GOV-07	Mechanism to: • Facilito recommen information	ns exist to establish contact with selected ate ongoing cybersecurity and privacy ed ded cybersecurity and privacy practices n including threats, vulnerabilities and ind	d groups and associed ducation and training techniques and tec cidents.	ations within the cybersecurity & privacy co g for organizational personnel; • Maintain c chnologies; and • Share current security-rel	urrency with ated	be Duje	12/27/2023	Edit
								Items per page:	15 ▼ 1 – 1 of 1	

Managing Controls Assigned to you, an Admin:

As an Admin, you'll have two options for managing your own controls, both of which are explained below.

- 1. **Option #1**
 - a. Click Assessment & Compliance (1)
 - b. Click Security Control Assessment (2)
 - c. Click on the desired framework from the dropdown menu (3)
 - d. Click on the desired Control Family name (4)
 - e. Mark the control to match its current state (5)
 - i. Control in Place
 - 1. The organization has an artifact or proof of concept for the chosen control.



2. For example, the policy or procedures are currently implemented in the organization and can be proven.

ii. Control Not in Place

- 1. The organization still needs to develop or work towards the desired control.
- 2. For example, the policies are not available thus the user needs to mark the control as not in place
- iii. Not Applicable
 - **1.** The control does not apply to the organization
- f. Provide the comments/answers as applicable under **Control Answer** (6)
- **g.** Upload an Artifact as applicable (7)
 - i. Click **Upload Artifacts**.
 - ii. Click the blue upload button.
 - iii. Choose the appropriate file and double-click on it.
 - iv. If you need to delete that file, check the box next to 'Name', click the 'X', then click 'OK' in the pop-up.
- h. Click Submit (8)

ASCENT PORTAL	Assessment & Compliance Governance Business Continuity Cybersecurit	y Vendor Management Reports At	oout Admin				Toe Duje (GILL Corp) 🧧
Admin Dashboard	WISP Framework						
🗄 Dashboard	Control Family Name	Score	Answered/Total	In Place	Not In Place	Not Applicable	Last Updated
Security Control Assessment	LCybersecurity & Privacy Governance	0%	0/1 - 00%	0	0	0	12/26/2023
	2. Asset Management	0%	0/1-00%	0	0	0	12/26/2023
Calendar	3. Cloud Security	0%	0/1-00%	0	0	0	12/26/2023
■ All Compliance Controls	4. Configuration Management	0%	0/2 - 00%	0	0	0	12/26/2023
	5. Continuous Monitoring	0%	0/3 - 00%	0	0	0	12/26/2023
➡ Controls Assigned to Me	6. Cryptographic Protections	0%	0/5 - 00%	0	0	0	12/26/2023
Control Evidence	7. Data Classification & Handling	0%	0/3 - 00%	0	0	0	12/26/2023
	8. Endpoint Security	0%	0/9 - 00%	0	0	0	12/26/2023
Artifact Library	9. Identification & Authentication	0%	0/11 - 00%	0	0	0	12/26/2023
	10. Mobile Device Management	0%	0/1-00%	0	0	0	12/26/2023
	II. Network Security	0%	0/3 - 00%	0	0	0	12/26/2023
	12. Privacy	0%	0/2 - 00%	0	0	0	12/26/2023
	13. Security Awareness & Training	0%	0/13 - 00%	0	0	0	12/26/2023
	14. Technology Development & Acquisition	0%	0/1 - 00%	0	0	0	12/26/2023
	15. Vulnerability & Patch Management	0%	0/2 - 00%	0	0	0	12/26/2023
	16. Web Security	0%	0/1 - 00%	0	0	0	12/26/2023
	17. Change Management	0%	0/2 - 00%	0	0	0	12/26/2023
					Items pe	r page: 50 ~ 1-	- 17 of 17 < >
0							



ASCENT PORTAL	Assessment & Compliance Governance Business Continuity Cybersecurity Vendor Management Reports About Admin Tool	Duje (GILL Corp) 🔒
Admin Dashboard	Back to Questionnaire	
- Dashboard	1 Cyberser uity & Privney Governmene	
Security Control Assessment		
Security & Compliance Calendar	GOV-07 Mechanisms exist to establish contact with selected groups and associations within the cybersecurity & privacy communities to: • Facilitate ongoing cybersecurity and privacy education and training for organizational personnel; • Maintain currency with recommended cybersecurity and privacy practices, techniques and technologies; and	
≡, All Compliance Controls	Share current security-related information including threats, vulnerabilities and incidents. Pending Auditor Approval	
E, Controls Assigned to Me	O Control in Place O Control Not in Place 5	
Control Evidence Documents (CEDs)	O Not Applicable Control Answer (if applicable)	
🚥 Artifact Library	6	
	Submit Upload Artifacts (1) Notes Assign (Ton Duje) 87	
	Back to Questionnaire	

- 2. *Option #2*
 - a. Click Assessment & Compliance (1)
 - b. Click **Controls Assigned to Me** (2)
 - c. Here you will see a list of controls assigned to you, which you can act on.

ASCENT PORTAL	Assessment & Comp	liance Governance	Business Continuity Cybe	ersecurity Vendor Management	t Reports Abou	t Admin				т	oe Duje (GILL	Corp) \varTheta
AP.	Security Control Fran	nework										
Admin Dashboard	WISP Framework		6									•
	Upcoming and Overc	due Controls										
	All Overdue											•
Assessment	Filter		*									
Security & Compliance	T men											-
Calendar	Control Family Name	Control ID	Control Description				Control Owner	Due Date	Action			
E All Compliance Controls									Items per page.	25 0 0	10 2	
E. Controls Assigned to Me	<u>~_0</u>								none por page.			
Control Evidence												
Documents (CEDs)												
🕶 Artifact Library												



Managing Controls Assigned to You, a User:

- **1.** Click **Assessment & Compliance** (1).
- 2. Click **Controls Assigned to Me** (2).
- 3. Here you will see a list of controls assigned to you, which you can act on.

ASCENT PORTAL	Assessment & Com	pliance Governance	e Business Continuity Cyb	ersecurity Vendor Manage	ment Reports A	oout Admin					Toe Duje ((GILL Corp)	0
Admin Dashboard	Security Control Fra	mework	0										
- Dashboard	Upcoming and Over	due Controls	U										
Security Control Assessment	Filter		Ŷ										
Calendar	Control Family	Control ID	Control Description				Control Owner	Due Date	Actio				
⇒ All Compliance Controls	Name								Items per page	25-	0 of 0		
E. Controls Assigned to Me	←2												
Control Evidence Documents (CEDs)													
Artifact Library													

Alerts to Help Manage Controls:

The automated alerts will help users stay on top of the tasks assigned to them, with several reminders along the way.

The person assigned to a control will receive the following alerts via email to help manage their to-do list:

- When a control has been assigned to them
- When a control is 5 days from being due
- When a control is 3 days from being due
- When a control is completed
- When a control is re-assigned to a new control owner

To view all upcoming and overdue controls:

- 1. Click Assessment & Compliance (1)
- 2. Click All Compliance Controls (2)
- 3. Click the drop-down to see **Upcoming and Overdue Controls** (3). This drop-down will show you controls that are:
 - a. Overdue
 - b. Due in 3 days
 - c. Due in 5 days
 - d. All tasks
- 4. The list will appear below the drop-down area (4).



ASCENT PORTAL	Assessment & Compliance Governan	nce Business Continuit	y Cybersecurity Vendor Management	Reports About A	dmin			Т	pe Duje (GILL	Corp) 😝
Admin Dashboard	Security Control Framework WISP Framework	` 1								•
- Dashboard										
Security Control	Control in Place		Control Not in Place		Overdue Control Tasks		Upcoming Contro (2023)	l Tasks		
Security & Compliance	Upcoming and Overdue Controls		61		0		1			
E All Compliance Controls	All Overdue									•
₽ Controls Assigned to Me	Filter	Ϋ́								•
Control Evidence Documents (CEDs)	Control Family Name Control ID	Control Desc	ription 🛧		Control Owner	Due Date	Action			
😂 Artifact Library	← 4						Items per page:	15 ▼ 0 o	(0 <	

Viewing and Managing Your to do List of Controls

To plan out your personal workload, you can view your upcoming controls to help you stay on top of your to-do list.

- 1. Click Assessment & Compliance (1)
- 2. Click **Controls Assigned to Me** (2)
- 3. Choose the framework from the drop-down menu (3)
- 4. Choose the filter you would like to view (4)
 - a. This drop-down will show you controls that are:
 - i. Overdue
 - ii. Due in 3 days
 - iii. Due in 5 days
 - iv. All tasks
- 5. View the list under **Control Family Name** (5)





Assigning Frameworks

- 1. Click **Admin** (1).
- 2. Click Manage Tenant (2).
- 3. From the list of tenants, locate and select the specific tenant for which you want to assign frameworks.
- Within the selected tenant's details find and click on **the number under** the Frameworks column (3).
- 5. To add a new framework, click the **plus sign** (4).
- 6. Create a survey name, add a description to help the team understand the purpose of the framework, and then choose the framework from the drop-down menu. Click **Submit**. (5)



ASCENT PORTAL	Assessment & Compliance Gover Filter	nance Business Continuity Cybersecurity Vendor Management Rep	orts About Admin		Ja	son Phillip (You	ng Partners LLC) 😌
🏦 Manage Tenant User	Framework Name	Template Name	Description	Туре	Controls	Status	Action
	ISO 27001 Security Assessment	ISO 27001 Security Assessment (New Version of Standard)	ISO 27001 Security Assessment (New Version of Standard)	control	144	Active	Edit
	HIPAA/HITECH/HITRUST CSF	HIPAA/HITECH/HITRUST CSF	HIPAA/HITECH/HITRUST CSF	control	1364	Active	Edit
				Items per	page: 15▼	1 - 2 of 2	

ASCENT PORTAL	Assessment & Compliance Governa	nce Business Continui	ty Cybersecurity Vendor N	fanagement Reports	About Admin			Jas	on Phillip (Youn	g Partners LLC)
Monage Tenant	Filter									+
🏄 Manage Tenant User	Framework Name	Template Name			Description		Туре	Controls	Status	Action
	ISO 27001 Security Assessment	ISO 27001 Security As	ssessment (New Version of S		ISO 27001 Security Assessment (Ne	w Version of Standard)	control	144	Active	Edit
	HIPAA/HITECH/HITRUST CSF	HIPAA/HITECH/HITRU	ST CSF		HIPAA/HITECH/HITRUST CSF		control	1364	Active	Edit
							items per	page: 15 *	1 - 2 of 2	
			Add Framework		×					
			Survey Name 5							
			Description	Please enter text	k					
			Survey Template		•					
					Submit					



Governance

Security Policies are the foundation of any organized, efficient Security Program. They dictate the control requirements for the organization.

Policies

In the Policies section of the Portal, you can create folders to organize the policies you upload.

- 1. Click Governance (1)
- 2. Click Policies (2)
- 3. Click the **folder icon** (3)
- 4. Name the folder (4) and click OK

ASCENT PORTAL	Ass		Toe Duje (GILL Corp)					
Policies	Filter						3 —	→00
A Incident Response			•					
Policies and Procedures Templates		Name		Created By		Created On S	lize (Kb)	Action
		Example Folder	(5	Toe Duje	1	12/26/2023		
					ite	ems per page: 10 -	1 - 1 0	n < >

ASCENT PORTAL	Asso	essment & Compliance Governance Business C	ontinuity Cybersecurity	Vendor Management Reports	About Admin			oe Duje (GILL Corp)	9
S Policies	Filter		٧					00) .
A Incident Response	•								
Policies and Procedures Templates		Name			Created By	Created On	Size (Kb)	Action	
		Example Folder			Toe Duje				
						items per page:	10-1		
				Add New Folder					
				Folder Name					
				Cancel Ok 4					
					_				

Templates

The Portal offers several templates to assist you when you are developing or revising your security environment. To access the templates:

- 1. Click Governance (1).
- 2. Click Policies and Procedures Templates (2).
- 3. Click **2023 Policies Templates** (3).
- 4. Here you will see a list of downloadable policies you can access and use at any time (4).



			The Daje (GILL Corp)
iter Ý			
↑ / 1			
] Name	Created By	Created On	Size (Kb) Action
] and a second	Whitehat Virtual admin	07/12/2023	
		Items per page:	10 - 1-1of1
Assessment & Compliance Governance Business Continuity Cybersecurity Vendor Management Re	eports About Admin		Toe Duje (GILL Corp)
ter 👻			
♠ / 2023 - Policies Template			
] Name	Created By	Created On	Size (Kb) Action
] AcceptableUsage Policy Template.docx	Whitehat Virtual admin	07/12/2023	79
AccessControl Policy Template docx	Whitehat Virtual admin	07/12/2023	38
Asset Management Policy template.docx	Whitehat Virtual admin	07/12/2023	30
Business Continuity and Disaster Recovery Policy Template.docx	Whitehat Virtual admin	07/12/2023	35
Change Management Policy Template.docx	Whitehat Virtual admin	07/12/2023	127
Cloud Security Policy Template.docx	Whitehat Virtual admin	07/12/2023	148
Cryptography and Encryption Policy Template.docx	Whitehat Virtual admin	07/12/2023	30
End Point Security Policy.docx	Whitehat Virtual admin	07/12/2023	148
Human Resources Security Policy template.docx	Whitehat Virtual admin	07/12/2023	30
Operations Security Policy Template.docx	Whitehat Virtual admin	07/12/2023	37
	Rer	Rer	Ref Created By Created On Azame Created By Created By Created On O/12/2023 Assert Scompliance Governance Business Continuity Cybersecurity Vendor Management Reports About Admin Assert Total Compliance Governance Business Continuity Cybersecurity Vendor Management Reports About Admin Assert Scompliance Governance Business Continuity Cybersecurity Vendor Management Reports About Admin Assert Management Scompliance Governance Business Continuity Cybersecurity Vendor Management Reports About Admin Assert Management Bacovernance Business Continuity Cybersecurity Vendor Management Reports About Admin Created Dy Created Dy Created Dy Created Dy Created Dy Created On Orthology Control

Incident Response

It is imperative to follow a detailed, prescribed process when navigating a security incident. By using the tools within the Portal, you and your team will be guided through the entire process from start to finish.

Incident Response Management

ASCENT Portal contains the capability to capture many incident response activities, including tracking and reporting.

How to track an incident in the Portal

- **1.** Click **Governance** (1)
- 2. Click Incident Response (2)
- **3.** Click the **+ sign** (3)
- 4. In the pop-up (4), the Portal will guide you through the information that needs to be documented.

ASCENT Portal Master User Guide



ASCENT PORTAL	Assessment & Compliance Governance	e Business Continuity Cybersecurity V	endor Management Reports About Admin			Toe Duje (GILL Corp) \varTheta
A Policies	Filter	× ×				3 → •
A Incident Response	Sequence Number	1 Date	Time Status	Owner Name	% Completed	Action
Policies and Procedures Templates	2				Items per page: 15▼	0 of 0 < >

ASCENT PORTAL	Assessment &	& Compliance Governance Business Continuity Cybers	security Vendor Management Reports About Admin				Toe Duje (0	SILL Corp) 🧲
R Policies	Filter	9						•
A Incident Response		Log New Incident		×	Completed	,	uction	
Policies and Procedures Templatas		Section 2: Incident Handler Section 2: Incident Reporter Section 3: Incident Details Section 4: Classification Of The Suspicious Activity Section 5: Host/Network Information Related To Incident Section 6: IP Address Of Suspected Source Section 7: Containment Section 8: Eradication Section 8: Recovery Section 10: Post-Mortem/Lessons Learned Incident Call Notes Documents	ATTESTATION: I understand that by submitting this Incident Report in good faith, I cannot be subject to retailation. I attest that the information contained in this Incident Report is true and accurate to the best of my knowledge on the date(s) indicated below. If I obtain any additional information regarding this Incident, I agree to provide said supplementary information immediately to the person specified as the designated incident Handler. I agree to cooperate fully with all investigators of this Incident unit the Incident is closed. DIRECTIONS: The reporting user or witness needs to provide as much detail as possible to complete this form. Please Note: All persons who contribute information to there port should be experiment to complete this form. Please Note: All persons who contribute information to there report should be report of the Incident All the answers are mandatory. Please enter the field's with "NA" if I is not applicable and In-line with the Incident Bandler. The completed form should be submitted with a 24 hours of discovery of the Incident All the answers are mandatory. Please enter the field's with "NA" if I is not applicable and In-line with the Incident. Mame ":		ser poge:	15+		



Chapter 4: Using the Portal MSP

Navigating the admin section

Within the **Admin tab** (1), you will be able to manage your own Portal for your MSP organization, as well as the customers, or tenants, that reside within the Portal under your organization.

Under **Type** (3), the type of account will be stated. This could be MSP (your organization), or End Client.

Under **Preference** (4), you can edit which day(s) of the week email notifications are sent out.

Under Action (5), you can edit the customer information (7).



ASCENT PORTAL	E Assessment	& Compliance G	overnance	Business Continuity Cyberse	curity Vendor Management Reports About Admin					Ann Marryl (T	Corp) \varTheta
A Manage Tenant	Tenant List										
	Filter					×			•	e	0
				Edit Client		^				-	
	Tenant ID	Name	Email ad	Client Name*	GILL Corp		Status	Preference	Action	Switch To	
			sheffali,	Email address*	sheffali jain@whitehatvirtual.com		Active	Edit	Edit	Swite	
	779		sheffali,	Service Tier	End Client .		Active	EG	Edt	Switz	
				Status	Active	i.		items per page:	15• 1		
				Time Zone	Central Standard Time	i.					
				Client Logo		5 I					
				Account Holder		i.					
				Street*	34798						
				City*	Austin						
				State*	Tennessee	•					
				Country	USA						
				Zip*	6788].					



By clicking **Switch** (6), you will switch to seeing that customer's Portal. This is especially helpful once you have many tenants under your own.

You will see which tenant Portal you are currently viewing by looking in the top right corner next to your name. In this example, we switched from TT Corp (the MSP) to GILL Corp (the tenant) (8).

ASCENT PORTAL	₽	Assessment & Compliance	About Admin						A	nn Marryl (Gl	LL Corp)
MSP Dashboard			Clients			Frameworks		Clients without active			T
Security Control Assessment			2			4		1			8
Security & Compliance Calendar	ŕ										
🖶 All Compliance Controls		GILL Corp			Na	me	Answered/Assigned	Assigned/Total			
E Controls Assigned to Me		NIST 800-171 rev2		0.00 / 0	Тое	a Duje	0.00%	100.00%			
Artifact Library											
		CMMC 2.0 Level 1		0.00 / 0							
		W/CD Framework		0.00 / 0							
		WISP Pramework		0.0070							
								Items per page: 3-	1-	1 of 1	
	1										

To switch back to the TT Corp Portal, click **Admin** (9), click **Manage Tenant** (10), then click **Switch** (11), which corresponds to the TT Corp line in the list.

ASCENT PORTAL	Assessment (& Compliance At	out Admin								Ann Marryl (GILL Corp)	0
Manage Tenant	10 Tesant List	/										
🏦 Manage Tenant User	Filter		Ϋ́								•	
Framework Subscription	Tenant ID	Name	Email address	State	Туре	Users	Frameworks	Status	Preference	Action	Switch To	
	780	GILL Corp	sheffali.jain@whitehatvirtual.com	Tennessee	End Client	4	4	Active	Edit	Edit	Switch	
	779	TT Corp	sheffali.jain@whitehatvirtual.com	Tennessee	MSP	2	<u>0</u>	Active	Edit	Edit	Switch	
									Items per page:	15-	1-2 of 2	
											(1)	

Upon signing in as the MSP admin, you will see a tenant for your own organization. In this example, it is TT Corp (1).

To add customers, or Tenants, under the MSP Portal, follow the below directions. In this example, the customer is GILL Corp (2).

Under the **Type** column, you can see if the account is the MSP or End User (3).

- 1. Click Admin (4)
- 2. Click Manage Tenant (5)
- 3. Click the plus sign (6)



ASCENT PORTAL	=	Assessment &	Compliance Gov	vernance I	Business Continuity Cybersecu	rity Vendor Managem	ent Reports A	oout Admin					Ann Marryl (TT Corp	p) \varTheta
🔁 Manage Tenant		Tenant List /							4					
1		Filter			Ϋ́							6 -	→ •	1
5		Tenant ID	Name	Email add	Iress	State	Туре	Users	Frameworks	Status	Preference	Action	Switch To	
		780 2	GILL Corp	sheffali.jo	ain@whitehatvirtual.com	Tennessee	End Client	4	4	Active	Edit	Edit	Switch	
		779 1	TT Corp	sheffali.jo	ain@whitehatvirtual.com	Tennessee	MSP	2	<u>Q</u>	Active	Edit	Edit	Switch	
											Items per page:	15• 1 -	2 of 2 <	
							3							
	-	Assessment & C	Compliance Gov	ernance B	Business Continuity Cybersecu	rity Vendor Manageme	ent Reports At	out Admin				Jason Philli	p (Young Partners LL	c) A
ASCENTIORIAL														
🕀 Manage Tenant		Tenant List /												
		Filler			Add New Client 7				×				•	
		Tenant ID	Name		Client Name*				A	Status	Preference	Action	Switch To	
			Young Partners	uc	Email address*					Active	Edit	Edit	Switch	
				3	Service Tier	MSP			•	Active	Edit	Edit	Switch	
			Capital Partners	s MSP	Status	Active				Active	Edt	Edit	Switch	
					Time Zone	Central Standard Time					Items per page:	15• 1 -	3 of 3 🦂	
					Client Logo									
					chent Logo									
			<u>_</u>	~	Account Holder									
				1	Whitelabel Code*									
			9-	~	Whitelabel CNAME									
					Street*									
					Olive .									
					City									
					State*				• •					

4. Fill in the information about the new user (7) and click **Submit**



How to edit tenant details

- 1. Click Admin (1)
- 2. Click Manage Tenant (2)
- 3. Click **Edit** under *Preference* column to edit the email frequency and type. (3)
- 4. Click Edit under Action column to edit the user information. (4)
- 5. Edit the information as needed and click Submit.

ASCENT PORTAL	Assessment	t & Compliance G	overnance Business Continuity Cybersecu	rity Vendor Managem	ent Reports /	About Admin					Ann Marryl (TT Corp)
🗭 Manage Tenant	Tenant List	T						•	•		
1	Filter		Ϋ́					S.	4		• •
	Tenant ID	Name	Email address	State	Туре	Users	Frameworks	Status	Preference	Action	Switch To
2	780	GILL Corp	sheffali.jain@whitehatvirtual.com	Tennessee	End Client	4	4	Active	Edit	Edit	Switch
	779	TT Corp	sheffali.jain@whitehatvirtual.com	Tennessee	MSP	2	٥	Active	Edit	Edit	Switch
									Items per page:	15•	1 - 2 of 2 < >

How to add users to a tenant

- 1. Log in to the Portal, which will log you in as the admin for your MSP organization (confirmed by the top right corner, which will state which organization you are logged in as) (0).
- 2. Click Admin (1).
- 3. Click Manage Tenant (2).
- 4. Click **Switch**, corresponding to the tenant you need to add a user to (3).

ASCENT PORTAL	₽	Assessment & 0	Compliance Go	vernance Business Continuity Cyb	bersecurity	Vendor Management	Reports A	About Admin						Ann Marryl (TT Corp)
Manage Tenant		Tenant List /							0					0
1		Filter		Ϋ́									3	• •
2	3	Tenant ID	Name	Email address		State	Туре	Users	F	Frameworks	Status	Preference	Action	Switch To
		780	GILL Corp	sheffali.jain@whitehatvirtual.com	n	Tennessee	End Client	4	4	4	Active	Edit	Edit	Switch
		779	TT Corp	sheffali.jain@whitehatvirtual.com	n	Tennessee	MSP	2	2	2	Active	Edit	Edit	Switch
												Items per page:	15• 1-	2 of 2 < >

- 5. You'll see the name in the top right corner has now switched to the tenant's account (4).
- 6. Click Admin (5).
- 7. Click Manage Tenant User (6).

a. Here you will see a list of the current users (7) and their user types (8).

8. Click the **plus sign** (9).



ASCENT PORTAL	Assessment & Co	ompliance About Admin					Ann Marryl (GILL Corp)
🤁 Manage Tenant	Filter 6	5					4 . 0
🚨 Manage Tenant User	User ID	Name 7	Email	User Type 8	Created On	Status	Action
Framework Subscription	675	Ann Marryl	ann.marryl@ttcorp.com	MSP Admin	12/26/2023	Active	Edit
	676	Toe Duje	Toe.duje@Gill.com	Tenant Admin	12/26/2023	Active	Edit
	677	Tom Cher	tom.cher@gill.com	Tenant User	12/26/2023	Active	Edit
	12	Whitehat Virtual admin	sheffali.jain@whitehatvirtual.com	Tenant Admin	05/07/2020	Active	Edit
					Iter	ms per page: 15 -	1 - 4 of 4 < >
	<u> </u>						

9. Add the new user's information (10) and access type (11) in the pop-up box and click Submit (12).

ASCENT PORTAL	Assessment & Cor	npliance About Admin						Ann Marryl (GILL Corp) \varTheta
🔁 Manage Tenant	Filter		÷						•••
21 Manage Tenant User	User ID	Name	En	nall	User Type	Created On	Status	Action	
E Framework Subscription		Ann Marryl	ar	nn.marryl@ttcorp.com	MSP Admin		Active	Edit	
	676	Toe Duje	Add New Tenant User	10	×	12/26/2023	Active	Edit	
	677	Tom Cher	rad field fending over	•		12/26/2023	Active	Edit	
		Whitehat Virtual adm	First Name			05/07/2020	Active	Edit	
			Last Name				items per page: 15+	1 - 4 of 4	< 2.
			Email						
			Time Zone	Central Standard Time	•				
			Status	Active	•				
			User Type 11		•				
			Access Type						
					12 Submit				

A welcome Email from the ASCENT Portal will be sent to the User with a link to set their password. The new user will need to follow the below directions:

- 1. The user will receive a welcome email from the ASCENT Portal.
- 2. Open the welcome email and click the password reset link within.
- 3. Follow the instructions on the password-setting page to create a new password for the user account.



How to assign frameworks to a tenant

- 1. Log in to the Portal, which will log you in as the admin for your MSP organization (confirmed by the top right corner, which will state which organization you are logged in as) (1).
- 2. Click Admin (2).
- 3. Click Manage Tenant (3).
- 4. Click **Switch**, corresponding to the tenant you need to add a user to (4).

ASCENT PORTAD	Assessmer Tenant List Filter	nt & Compliance G	overnance Business Continuity Cybersecu	ity Vendor Managen	ent Reports A	About Admin	2			4	Ann Marryl (TT Corp)
	Tenant ID	Name	Email address	State	Туре	Users	Frameworks	Status	Preference	Action	Switch To
•	780	GILL Corp	sheffali.jain@whitehatvirtual.com	Tennessee	End Client	4	5	Active	Edit	Edit	Switch
	779	TT Corp	sheffali.jain@whitehatvirtual.com	Tennessee	MSP	2	<u>0</u>	Active	Edit	Edit	Switch
									Items per page:	15• 1 -	- 2 of 2 < >

- 5. Now that you are in the tenant's Portal (confirmed in the top right corner by stating the company's name) (5), click **Admin** (6).
- 6. Click Framework Subscription (7).
 - a. Here you will see the current frameworks assigned to this Portal and details for each framework.

ASCENT PORTAL	Assessment & Compliance About	Admin					Ann Marryl (GILL Corp) 😫
🔁 Manage Tenant	Filter	Ŷ					•
🚨 Manage Tenant User	Framework Name	Template Name	Description	Туре	Controls	Status	Action
Framework Subscription	WISP Framework	WISP Framework 2.0	WISP Framework 2.0	wisp	61	Active	Edit
	CMMC 2.0 Level 1	US CMMC 2.0 Level 1		control	25	Active	Edit
	NIST 800-171 rev2	NIST 800-171 rev 2		control	224	Active	Edit
	ISO27001-v2022	ISO 27001 v2022		control	48	Active	Edit
					iten	ns per page: 15 - ∙	1 - 4 of 4 < >

7. Click the **plus sign** (8).

ASCENT PORTAL	Assessment & Compliance Abo	ut Admin					Ann Marryl (GILL Corp)
🕬 Manage Tenant	Filter						6 0
22 Manage Tenant User	Framework Name	Template Name	Description	Туре	Controls	Status	Action
Framework Subscription	WISP Framework	WISP Framework 2.0	WISP Framework 2.0	wisp	61	Active	Edit
	CMMC 2.0 Level 1	US CMMC 2.0 Level 1		control	25	Active	Edit
T	NIST 800-171 rev2	NIST 800-171 rev 2		control	224	Active	Edit
7	ISO27001-v2022	ISO 27001 v2022		control	48	Active	Edit
	Test Framework	NIST 800-171 rev 2		control	224	Active	Edit
					Items	per page: 15•	1 - 5 of 5 < >



8. In the pop-up box, type in the framework name you'd like associated with the framework template (9), a description (10), and then select the desired framework (11) from the dropdown menu and click **Submit** (12).

ASCENT PORTAD	Assessment & Compliance About Admin						A	nn Marryl (GILL Corp) 🤒
🔁 Manage Tenant	Filter	Ŷ						•
🏦 Manage Tenant User	Framework Name	Template Name		Description	Туре	Controls	Status	Action
H Framework Subscription	WISP Framework	WISP Framework 2.0		WISP Framework 2.0	wisp		Active	Edit
	CMMC 2.0 Level 1	US CMMC 2.0 Level 1	Ð				Active	Edit
	NIST 800-171 rev2	NIST 800-171 rev 2				224	Active	Edit
		ISO 2700	te Client Survey	×	control	48	Active	Edit
	Test Framework	NIST BOD		~	control	224	Active	Edit
		Survey	y Name 9 Test F	ramework		items per p	xage: 15 • 1 − 5	
		Descrip	iption 10 Pleas	e enter text				
		Status	Active	•				
				12 Submit				

You'll see the newly assigned framework now in the list (13).

ASCENT PORTAL	Assessment & Compliance About Admin						Ann Marryl (GILL Corp)
Hanage Tenant	Filter	¥					•
21 Manage Tenant User	Framework Name	Template Name	Description	Туре	Controls	Status	Action
Framework Subscription	WISP Framework	WISP Framework 2.0	WISP Framework 2.0	wisp	61	Active	Edit
	CMMC 2.0 Level 1	US CMMC 2.0 Level I		control	25	Active	Edit
	NIST 800-171 rev2	NIST 800-171 rev 2		control	224	Active	Edit
	ISO27001-v2022	ISO 27001 v2022		control	48	Active	Edit
	Test Framework	NIST 800-171 rev 2		control	224	Active	Edit
	K				Items per	oage: 15 - 1-	5 of 5 < >
	13						



How to deactivate a framework for a tenant

- 1. Log in to the Portal, which will log you in as the admin for your MSP organization (confirmed by the top right corner, which will state which organization you are logged in to) (1).
- 2. Click Admin (2).
- 3. Click **Manage Tenant** (3).
- 4. Click **Switch**, corresponding to the tenant you need to access (4).

ASCENT PORTAL	Filte	Assessment & (enant List /	Compliance Go	vernance Business Continuity Cybersecurity	Vendor Managem	ent Reports .	About Admin	2			4	Ann Marryl	(TT Corp)
	Ter	ant ID	Name	Email address	State	Туре	Users	Frameworks	Status	Preference	Action	Switch	То
	780)	GILL Corp	sheffali.jain@whitehatvirtual.com	Tennessee	End Client	4	5	Active	Edit	Edit	Sv	vitch
	779	E.	TT Corp	sheffali.jain@whitehatvirtual.com	Tennessee	MSP	2	<u>0</u>	Active	Edit	Edit	Sv	vitch
										Items per page:	15• 1	1 – 2 of 2	

- 5. Now that you are in the tenant's Portal (confirmed in the top right corner by stating the company's name (5), click **Admin** (6).
- 6. Click **Framework Subscription** (7).
 - a. Here you will see the current frameworks assigned to this Portal, and details for each framework.
- 7. Click **Edit** next to the corresponding framework that needs to be deactivated (8).

ASCENT PORTAL	Assessment & Compliance Ab	out Admin					Ann Marryl (GILL C	Sorp) \varTheta
Manage Tenant	Filter	* 6					5	•
22 Manage Tenant User	Framework Name	Template Name	Description	Туре	Controls	Status	Action	T
E Framework Subscription	WISP Framework	WISP Framework 2.0	WISP Framework 2.0	wisp	61	Active	Edit	
	CMMC 2.0 Level 1	US CMMC 2.0 Level 1		control	25	Active	Edit	8
Т	NIST 800-171 rev2	NIST 800-171 rev 2		control	224	Active	Edit	
7	ISO27001-v2022	ISO 27001 v2022		control	48	Active	Edit	
•	Test Framework	NIST 800-171 rev 2		control	224	Active	Edit	
					item	s per page: 15 v	1 - 5 of 5 <	

8. Click the Status dropdown and choose Inactive, then click Submit (9).



ASCENT PORTAL	Assessment & Compliance About Admin						Ann Marryl (GILL Corp) 🔒
	Filter	¥					•
	Framework Name	Template Name	Description	Туре	Controls	Status	Action
Framework Subscription	WISP Framework	WISP Framework 2.0	WISP Framework 2.0	wisp		Active	Edi
	CMMC 2.0 Level 1	US CMMC 2.0 Level 1		control	25	Active	Edit
	NIST 800-171 rev2	NIST 800-171 rev 2		control	224	Active	Edit
		ISO 27007		control	48	Active	Edit
	Test Framework	NIST 800-		control	224	Active	Edit
		Survey Name	WISP Framework		Items per	page: 15 + 1-	5 of 5 < 🕹
		Description	WISP Framework 2.0				
		Status	Inactive				
		9	Submit				

9. Confirm the framework is inactive by checking the status in the list of frameworks (10).

ASCENT PORTAL	Assessment & Compliance Ab	out Admin				10	Ann Marryl (GILL Corp)
Hanage Tenant	Filter	Ψ				Ĭ	•
🚨 Manage Tenant User	Framework Name	Template Name	Description	Туре	Controls	Status	Action
R Framework Subscription	WISP Framework	WISP Framework 2.0	WISP Framework 2.0	wisp	61	Inactive	Edit
	CMMC 2.0 Level 1	US CMMC 2.0 Level 1		control	25	Active	Edit
	NIST 800-171 rev2	NIST 800-171 rev 2		control	224	Active	Edit
	ISO27001-v2022	ISO 27001 v2022		control	48	Active	Edit
	Test Framework	NIST 800-171 rev 2		control	224	Active	Edit
					Item	s per page: 15 ▼	1 – 5 of 5 < >

How to set access types for a new user within a tenant

- 1. Log in to the Portal, which will log you in as the admin for your MSP organization (confirmed by the top right corner, which will state which organization you are logged in to) (1).
- 2. Click Admin (2).
- 3. Click Manage Tenant (3).
- 4. Click **Switch**, corresponding to the tenant you need to access (4).

ASCENT PORTAL	=	Assessment &	Compliance Go	vernance Business Continuity Cybersecurity	Vendor Manageme	nt Reports Al	out Admin					Ann Marryl (TT Corp)	•
🔁 Manage Tenant		Tenant List /										1	
1		Filter		Ψ			2				4	• •	
		Tenant ID	Name	Email address	State	Туре	Users	Frameworks	Status	Preference	Action	Switch To	
e		780	GILL Corp	sheffali.jain@whitehatvirtual.com	Tennessee	End Client	4	5	Active	Edit	Edit	Switch	
		779	TT Corp	sheffali.jain@whitehatvirtual.com	Tennessee	MSP	2	٥	Active	Edit	Edit	Switch	
										Items per page:	15• 1-3	2 of 2 < >	

- 5. Now that you are in the tenant's Portal (confirmed in the top right corner by stating the company's name) (5), click **Admin** (6).
- 6. Click Manage Tenant User (7).
- 7. Click the **plus sign** (8).



ASCENT PORTAL 7	Assessment & Com	pliance About Admin					Ann Marryl (GILL Corp)
Manage Tenant	Filter	Ť					
💒 Manage Tenant User	User ID	Name	Email	User Type	Created On	Status	Action
Framework Subscription	675	Ann Marryl	ann.marryl@ttcorp.com	MSP Admin	12/26/2023	Active	Edit
an 25 ann an 100 an 200 ann a' Anna an 1	676	Toe Duje	Toe.duje@Gill.com	Tenant Admin	12/26/2023	Active	Edit
	677	Tom Cher	tom.cher@gill.com	Tenant User	12/26/2023	Active	Edit
	12	Whitehat Virtual admin	sheffali.jain@whitehatvirtual.com	Tenant Admin	05/07/2020	Active	Edit
					ltems per	page: 15 -	1 – 4 of 4 < >

- 8. Fill in the user's information (9).
- 9. Choose the User Type that will correspond to the user's access levels (10). The choices are:
 - a. Tenant Admin
 - i. Only Tenant admins can add other users to the tenant
 - b. Tenant User
 - c. Auditor
 - d. MSP Admin
 - e. Carrier Admin
 - f. Broker Admin
 - g. Agent Admin
 - h. Policyholder Admin
 - i. Policyholder User
 - j. Subsidiary Admin
- 10. Click **Submit** (11).

ASCENT PORTAL	=	Assessment & Comp	bliance About Admin								Ann Marryl (GILL Corp) 🔒
		Filter		Ŷ								+
22 Manage Tenant User		User ID	Name		Ema	a .	User Type	Created On	Status		Action	
		675	Ann Marryl		ann	.marryl@ttcorp.com	MSP Admin		Active		Edit	
			Toe Duje	Add New Tena	nt User	9	******	12/26/2023	Active		Edit	
		677	Tom Cher					12/26/2023	Active		Edit	
			Whitehat Virtual adm	First Name				05/07/2020	Active		Edit	
				Last Name					items per page:	15• 1	- 4 of 4	81 8
				Email								
				Time Zone		Central Standard Time	-					
				Status		Active	-					
				User Type	10		-	9				
				Access Type			•					
							11 Submit					

11. A new user email will be sent to the new user from the Portal.



How to export Tenant details in excel format

To pull an excel report of the tenants and users within the tenants, follow these steps:

- 1. Click Admin (1).
- 2. Click Manage Tenant User (2).
- 3. Click the **export icon** (3).
- 4. An excel file will download to your downloads folder.

ASCENT PORTAL	Assessment &	Compliance Governance Business Con	inuity Cybersecurity Vendor Management Reports Abou	Admin			Ann Marryl (TT Corp) \varTheta
Manage Tenant User	Filter	Ŷ						•
•	User ID	Name	Email	User Type	Created On	Status	Action	T
	675	Ann Marryl	ann.marryl@ttcorp.com	MSP Admin	12/26/2023	Active	Edit	
2	12	Whitehat Virtual admin	sheffali.jain@whitehatvirtual.com	Tenant Admin	05/07/2020	Active	Edit	3
					Ite	erns per page: 15♥	1 – 2 of 2	

How to view a compliance score of a tenant

- 1. Click Admin (1)
- 2. Click Manage Tenant (2)
- 3. Click **Switch** (3) associated with the tenant you would like to review.
- 4. Click Assessment & Compliance (4)
- 5. Click **MSP Dashboard** (5)
- 6. You also can now view the score from this MSP Dashboard.

ASCENT PORTAL	Asses:	ment & Compliance	Sovernance Business Continuity Cybersecu	rity Vendor Managem	ent Reports	About Admin					Ann Marryl (TT Corp)
A Manage Tenant	Tenan	:List /				K					
1	Filter		¥							3	• •
	Tenant ID	Name	Email address	State	Туре	Users	Frameworks	Status	Preference	Action	Switch To
2	780	GILL Corp	sheffali.jain@whitehatvirtual.com	Tennessee	End Client	4	5	Active	Edit	Edit	Switch
	779	TT Corp	sheffali.jain@whitehatvirtual.com	Tennessee	MSP	2	<u>0</u>	Active	Edit	Edit	Switch
									Items per page:	15 • 1	- 2 of 2 💎 🔿



ASCENT PORTAL	₽	Assessment & Compliance	About Admin							A	nn Marryl (G	ILL Corp) \varTheta
MSP Dashboard Security Control Assessment	1		Clients 2			Frameworks	۵	Clients without active framework				
Calendar												
E All Compliance Controls		GILL Corp			N	ame	Answered/Assigned		Assigned/Total			
➡, Controls Assigned to Me		ISO27001-v2022		0.00 / 0			0.00%		100.001			
Artifact Library		NIST 800-171 rev2		0.00 / 0								
		CMMC 2.0 Level 1		0.00 / 0								
	L								Items per page: 3•	• 1-	1 of 1	

How to create a summary of compliance scores for all tenants

- 1. Log in to your tenant (1).
- 2. Click Assessment & Compliance (2).
- 3. Click **MSP Dashboard** (3).
- 4. Here you will be able to see the compliance score of all the tenants.

Image: Mass Dashboard Clients Image: Trameworks Image: Clients without active framework Image: Clients without active fram	Ann Marryl (TT Corp)		About Admin	r Management Reports	Cybersecurity Vend	ernance Business Continuity	Assessment & Compliance	ASCENT PORTAL
		Clients without active framework		Frameworks 4		nts	10	MSP Dashboard
B Security Control 3							3	Security Control Assessment
Security & Compliance Gill Corp Name Answered/Assigned Assigned/Total		Assigned/Total	Answered/Assigned	Name			GILL Corp	Calendar
Ex. All Compliance Controls 15027001-v2022 0.00 / 0 100.00% 100.00%		100.00%	0.00%	Toe Duje	0.00 / 0		ISO27001-v2022	E All Compliance Controls
E, Controls Assigned to Me								E, Controls Assigned to Me
Control Evidence Documents (CEDe)					0.00 / 0		NIST 800-171 rev2	Control Evidence Documents (CEDs)
CMMC 2.0 Level 1 0.00 / 0					0.00 / 0		CMMC 2.0 Level 1	ன Artifact Library
Risk Assessment								👔 Risk Assessment
✓ Acknowledgements	1-1011 ()	Items per page: 3						 Acknowledgements

How to set overdue control automatic email frequency for a tenant

- 1. Log in to your tenant (1).
- 2. Click Admin (2).
- 3. Click Manage Tenant (3).
- 4. Select any Tenant and click on **Edit**, listed under the **Preferences** column (4).



ASCENT PORTAL	E As	ssessment & Co nant List /	mpliance G	overnance Business Continuity Cybersecurity	Vendor Managem	eent Reports	About Admin					Ann Marryl (TT Corp)
1	Filter			¥				2	4			• •
	Tena	nt ID	Name	Email address	State	Туре	Users	Frameworks	Status	Preference	Action	Switch To
3	780		GILL Corp	sheffali.jain@whitehatvirtual.com	Tennessee	End Client	4	5	Active	Edit	Edit	Switch
	779		TT Corp	sheffali.jain@whitehatvirtual.com	Tennessee	MSP	2	٥	Active	Edit	Edit	Switch
										items per page	: 15•	1 – 2 of 2 < >

5. In the pop-up, choose which day(s) the Portal will be allowed to email overdue control alerts to users, and click **Submit** (5).

ASCENT PORTAL		Assessment &	Compliance Go	vernance I	Business Continuity Cybersecurit	y Vendor Managem	ent Reports	About Admin				A	nn Marryl (TT Co	orp) \varTheta
Manage Tenant		Tenant List /												
		Filter			¥								•	•
		Tenant ID	Name	Email add	lress	State	Туре	Users	Frameworks	Status	Preference	Action	Switch To	
			GILL Corp	sheffali.j	Preferences				×	Active	Edit	Edit	Switch	
		779	TT Corp	sheffali.j	Overdue Mail Frequency	-				Active	Edit	Edit	Switch	
					General			Weekday			Items per page:	15 . 1 - 2 o		
								Tueday						
								Wednesday						
								Thursday						
						0		Friday						
								Saturday						
								Sunday						
								6						
								5	Submit					

How to add an Internal/External Auditor to the Portal

- 1. Log in to your tenant (1).
- 2. Click Admin (2).
- 3. Click **Manage Tenant** (3).
- 4. Click the number listed under the Users column (4).

ASCENT PORTAL	Assess	ment & Compliance G	overnance Business Continuity Cybersecu	rity Vendor Managem	ent Reports /	bout Admin					Ann Marryl (TT Corp) \varTheta
Manage Tenant	Tenant	List /				K					
1	Filter		¥			2					• •
3	Tenant ID	Name	Email address	State	Туре	Users 4	Frameworks	Status	Preference	Action	Switch To
	780	GILL Corp	sheffali.jain@whitehatvirtual.com	Tennessee	End Client	4	5	Active	Edit	Edit	Switch
	779	TT Corp	sheffali.jain@whitehatvirtual.com	Tennessee	MSP	2	٥	Active	Edit	Edit	Switch
									Items per page:	15• 1	- 2 of 2 < >

5. Click the **plus icon** to add a new user (5).



iant Te	enant List	/ GILL Corp /						
Filte	èr		Ÿ				5 -	\rightarrow
Use	er ID	Name	Email	User First Name	User Type	Created On	Status	Action
675	5	Ann Marryl	ann.marryl@ttcorp.com	Ann	MSP Admin	12/26/2023	Active	Edi
676	5	Toe Duje	Toe.duje@Gill.com	Тое	Tenant Admin	12/26/2023	Active	Edi
677	'	Tom Cher	tom.cher@gill.com	Tom	Tenant User	12/26/2023	Active	Edi
12		Whitehat Virtual admin	sheffali.jain@whitehatvirtual.com	Whitehat	Tenant Admin	05/07/2020	Active	Edi

6. Fill in the new auditor's information, and under **User Type**, choose **Auditor** (6). Click **Submit** (7).

ASCENT PORTAL	E Assessmen	& Compliance Governance	Business Continuity Cybersed	urity Vendor Management Reports About Admin				Ann Marryl (TT Corp) 😫
🔁 Manage Tenant	Tenant List	/ GILL Corp /						
	Filter		¥					•
	User ID	Name	Add New Tenant User		×	Created On	Status	Action
	675	Ann Marryl			_		Active	Edit
	676	Toe Duje	First Name		_		Active	Edit
	677	Tom Cher	Last Name				Active	Edit
		Whitehat Virtual admin	Title				Active	Edit
			Email			Items per page:	15• 1	- 4 of 4 💦 🗇
			Time Zone	Central Standard Time	•			
			Status	Active	•			
			User Type	Auditor	•			
			Access Type		•			
				6 7 Subr	mit			