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?
    - 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**
    - 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 well-being.

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 sales@ASCENT-Portal.com. 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

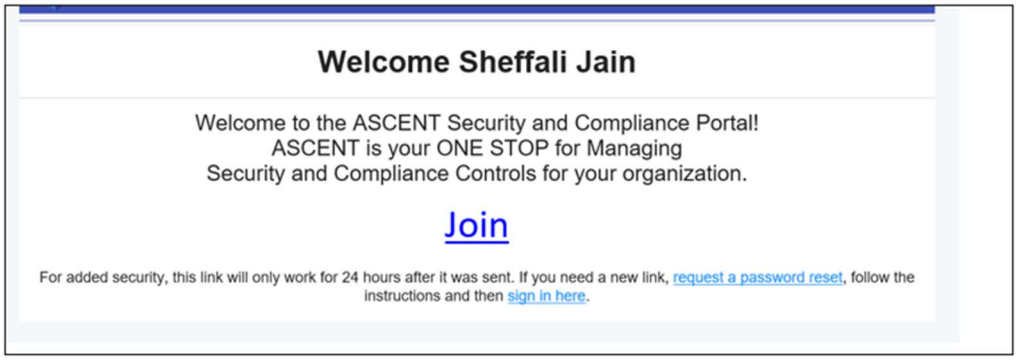
What kind of support or assistance does ASCENT Portal provide in case of security incidents or breaches?

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 Support@ASCENT-Portal.com where you can directly connect with the Security team.

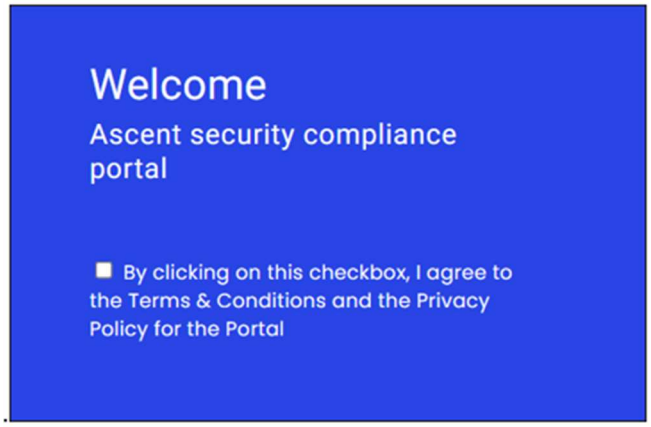
Chapter 2: Getting Started

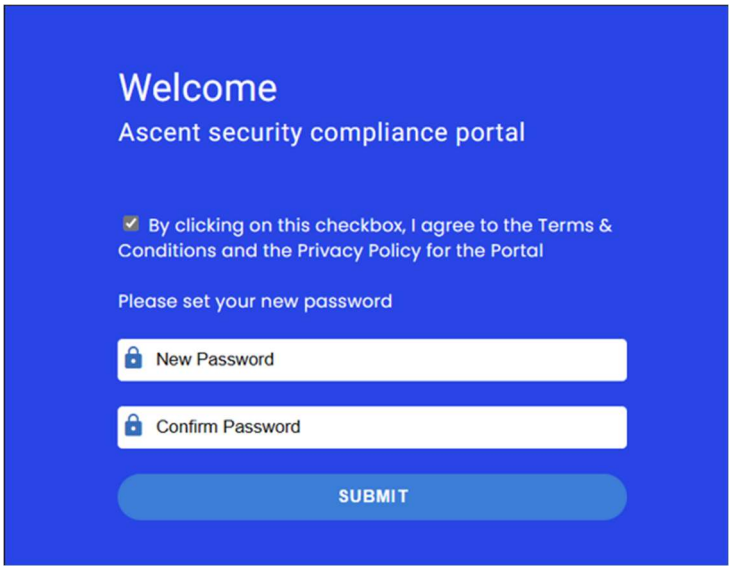
Getting signed up and logged in for the first time

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



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





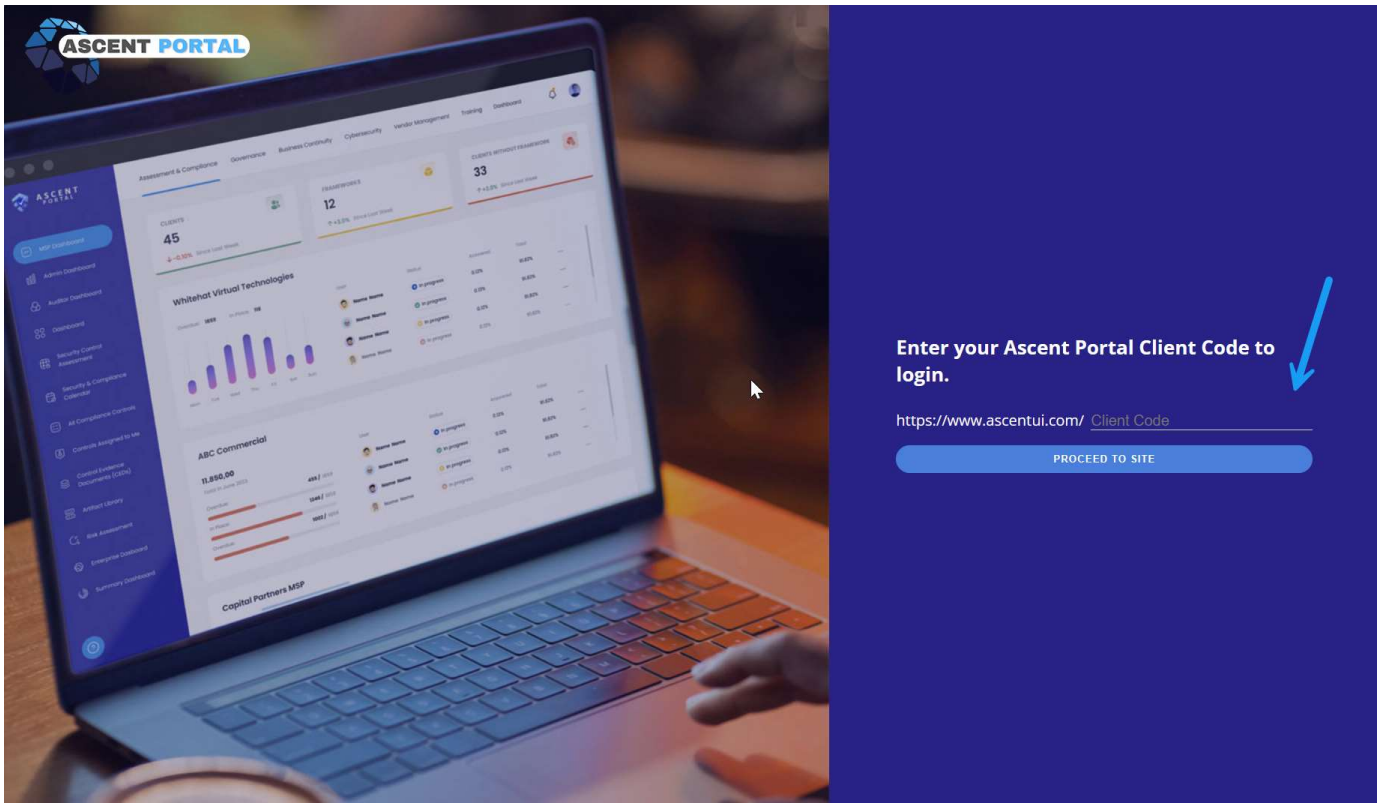
Here is a direct link to the Portal: ascentui.com

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

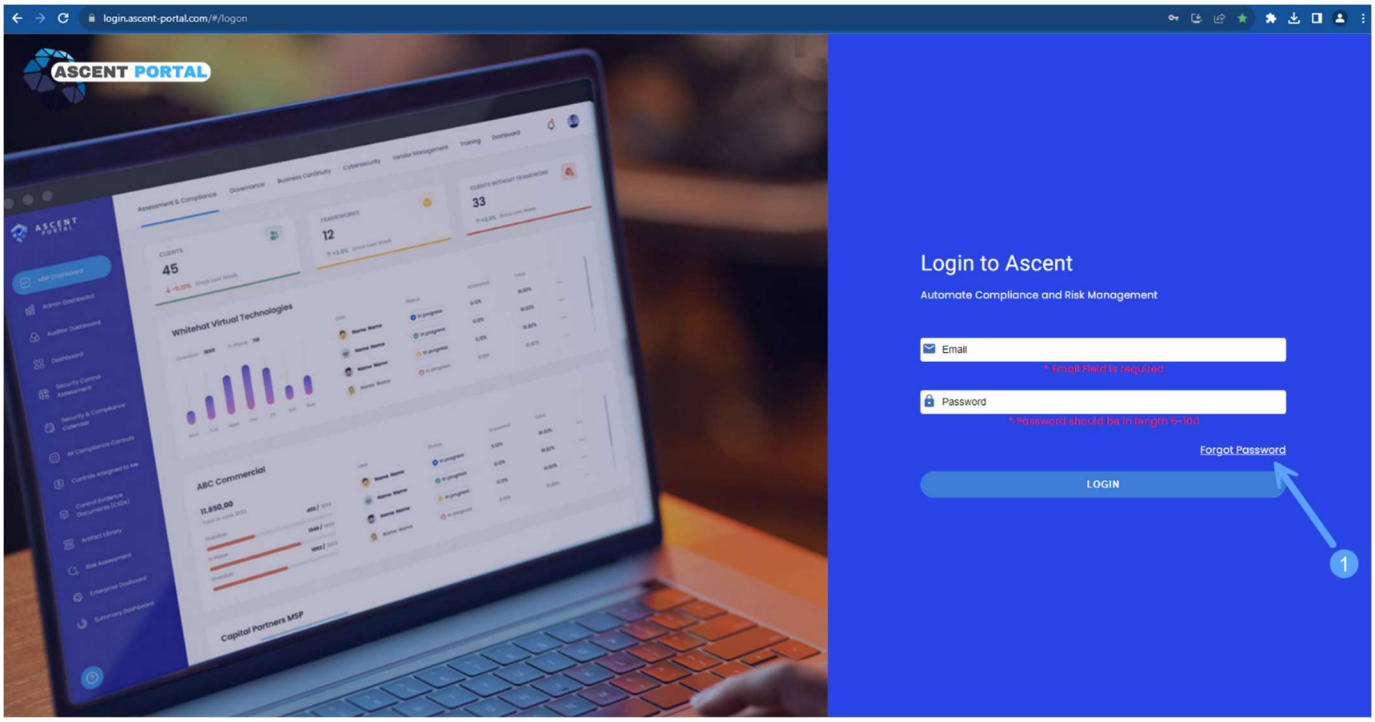
How to reset your password

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

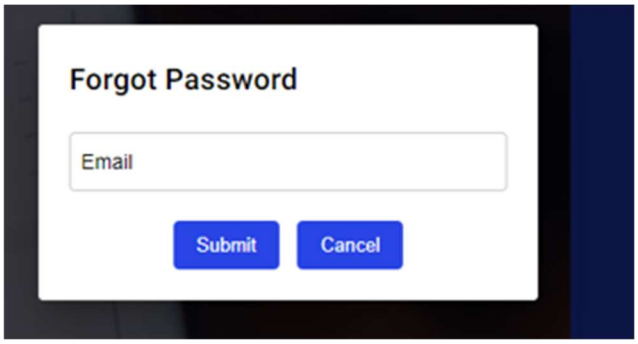
1. Follow this link to the Portal: ascentui.com
2. On the login page, you will first be asked to enter your **Ascent Portal Client Code**, this is the name of your organization.

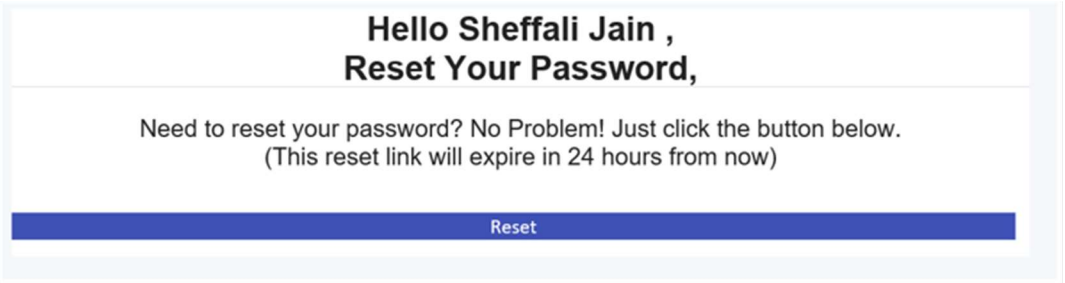


3. Once you pass this page you will see the login screen that will ask for your **Email and Password**. Click on the **Forgot Password link** seen in the image below.
4. Enter the email address associated with your user credentials. If you are unsure about your user credentials, please contact support@ASCENT-Portal.com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



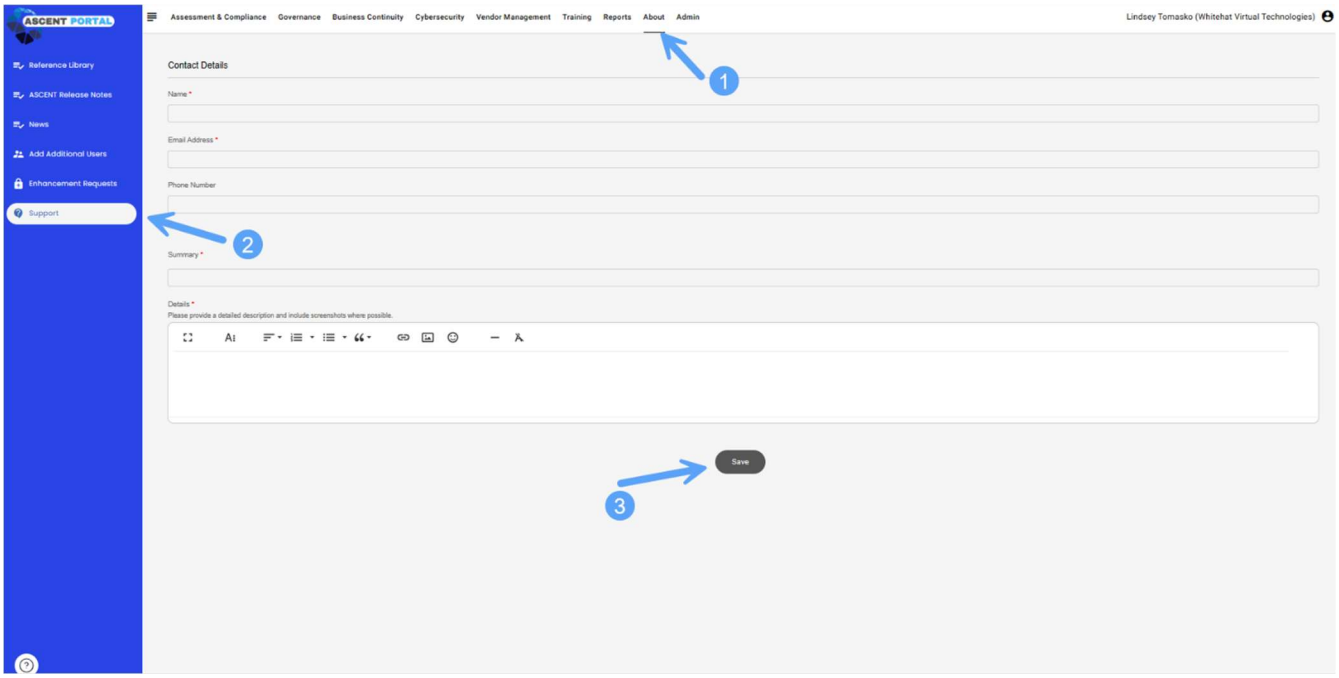


How to get support for the Portal

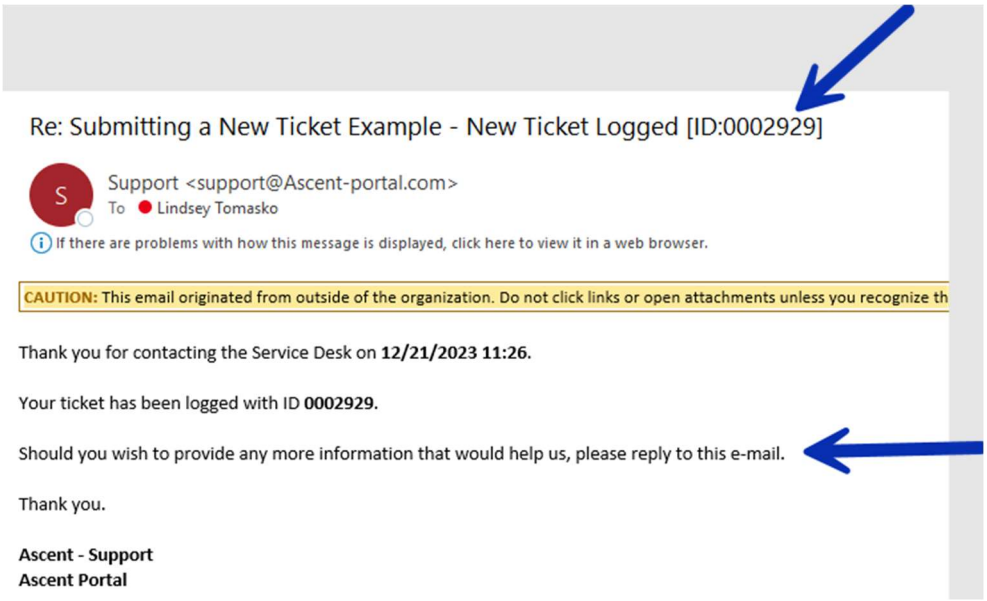
If you need support with functionality of the Portal, logging in, or other Portal-related issues, please log a ticket with our support team.

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.



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.



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.

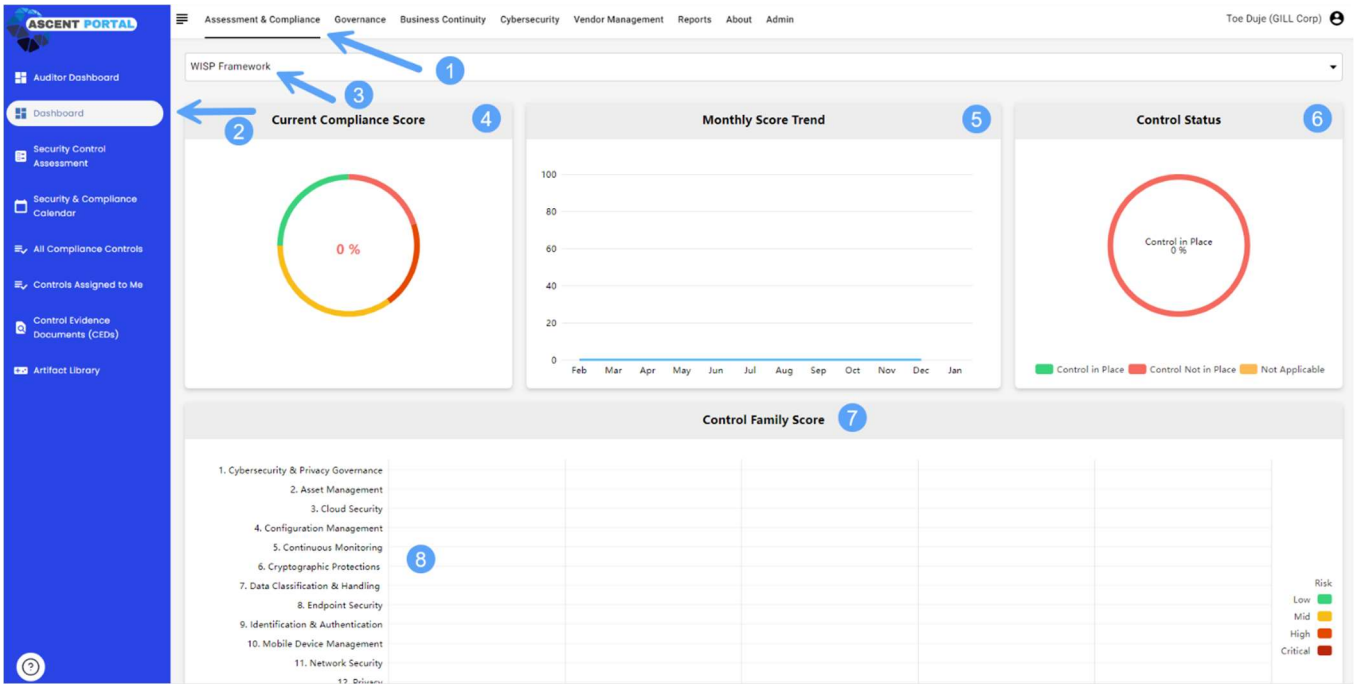
Current Compliance Score (4) - Use the Current Compliance Score to get an instant overview. Green indicates areas in compliance, yellow signals attention needed soon, and red flags areas out of compliance requiring immediate attention.

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.

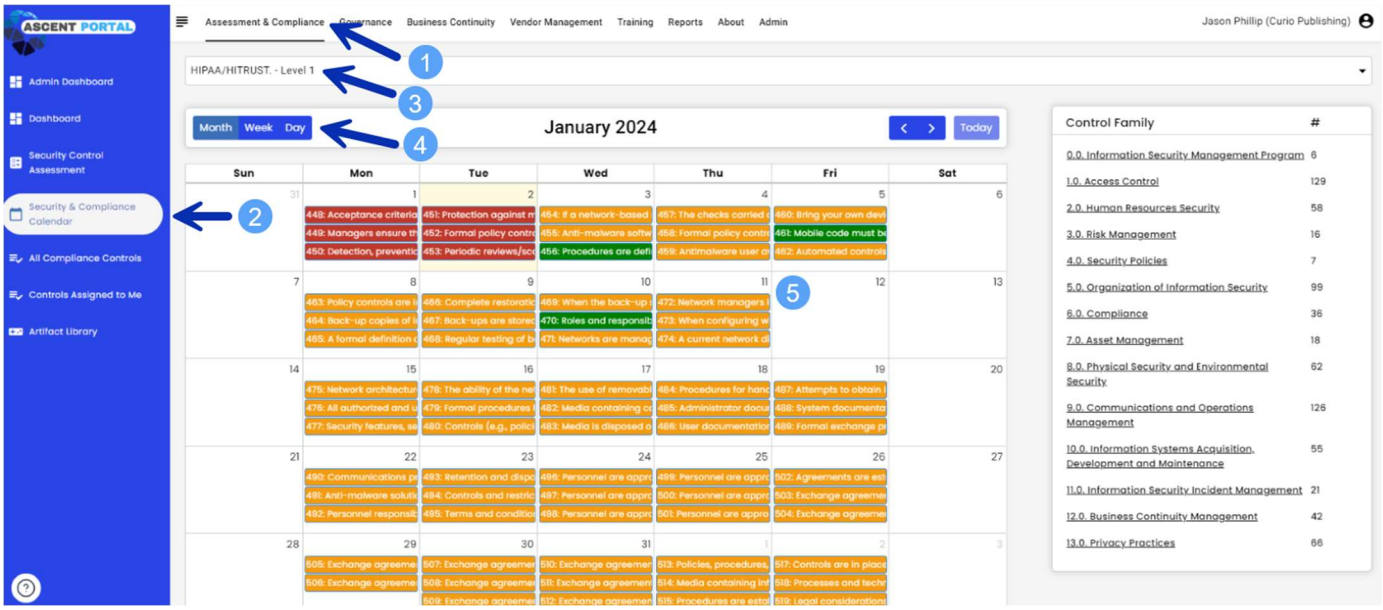
Calendar

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



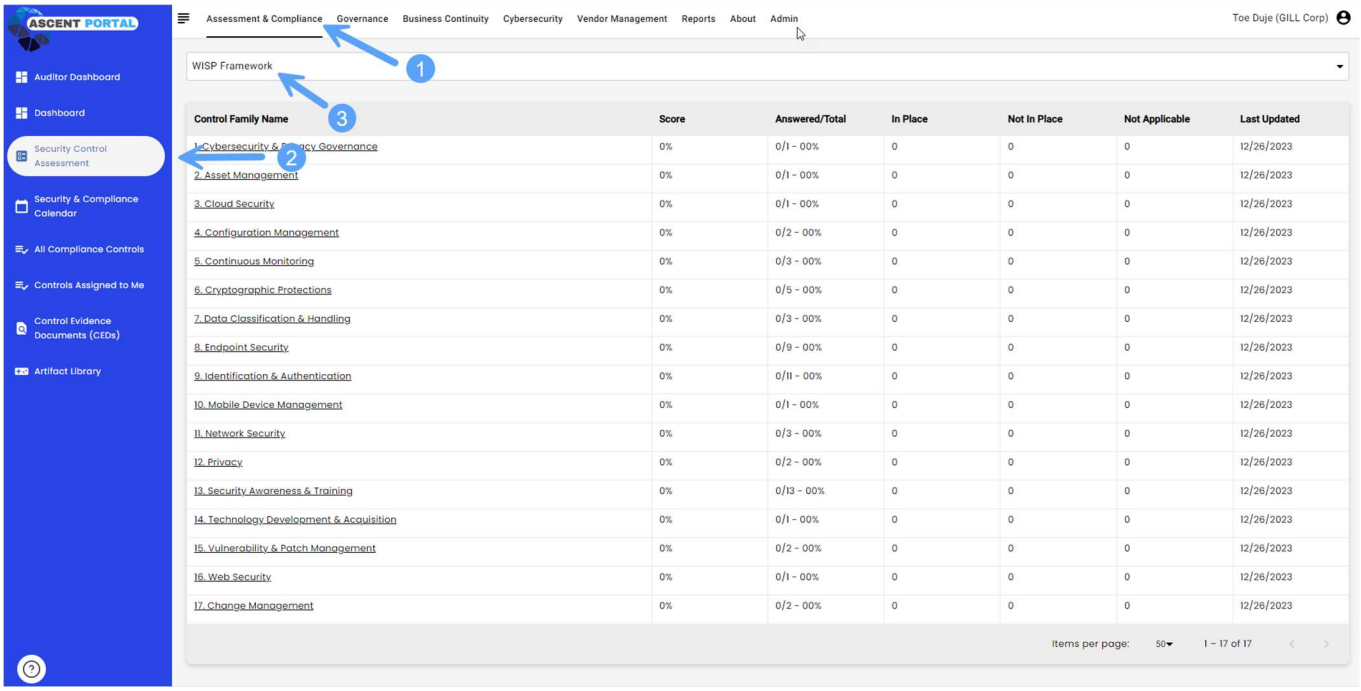
Artifacts

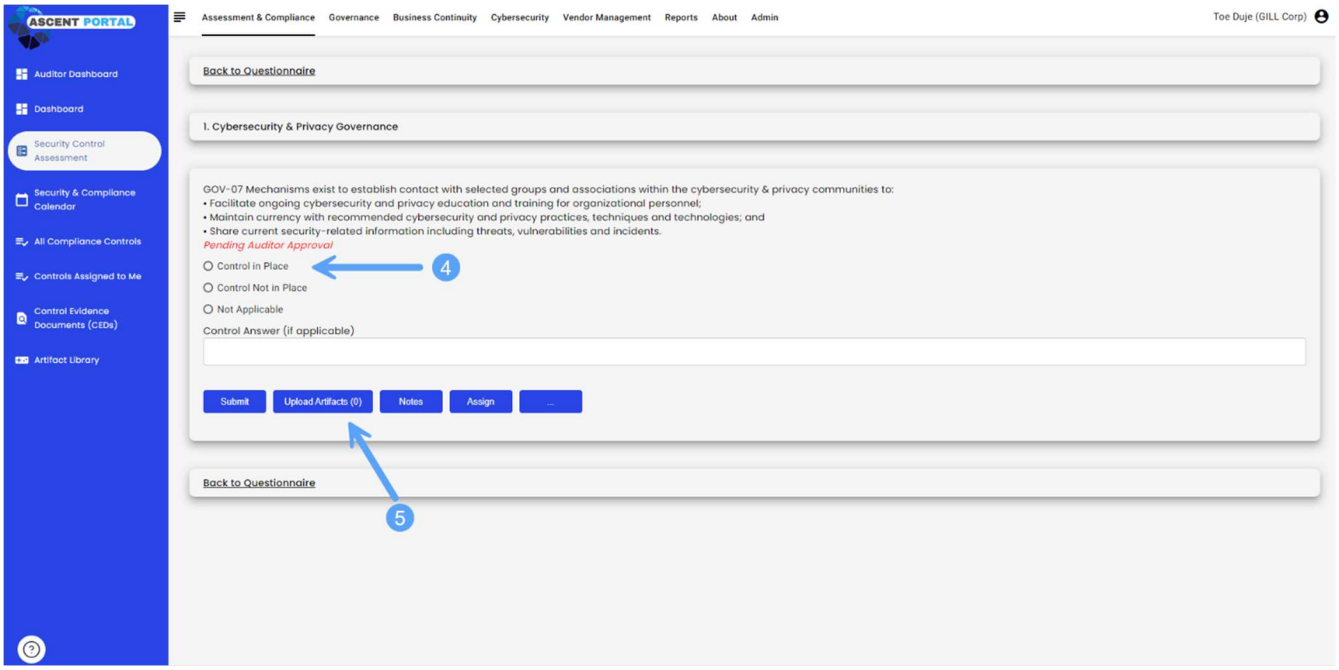
What is an artifact and what is its purpose?

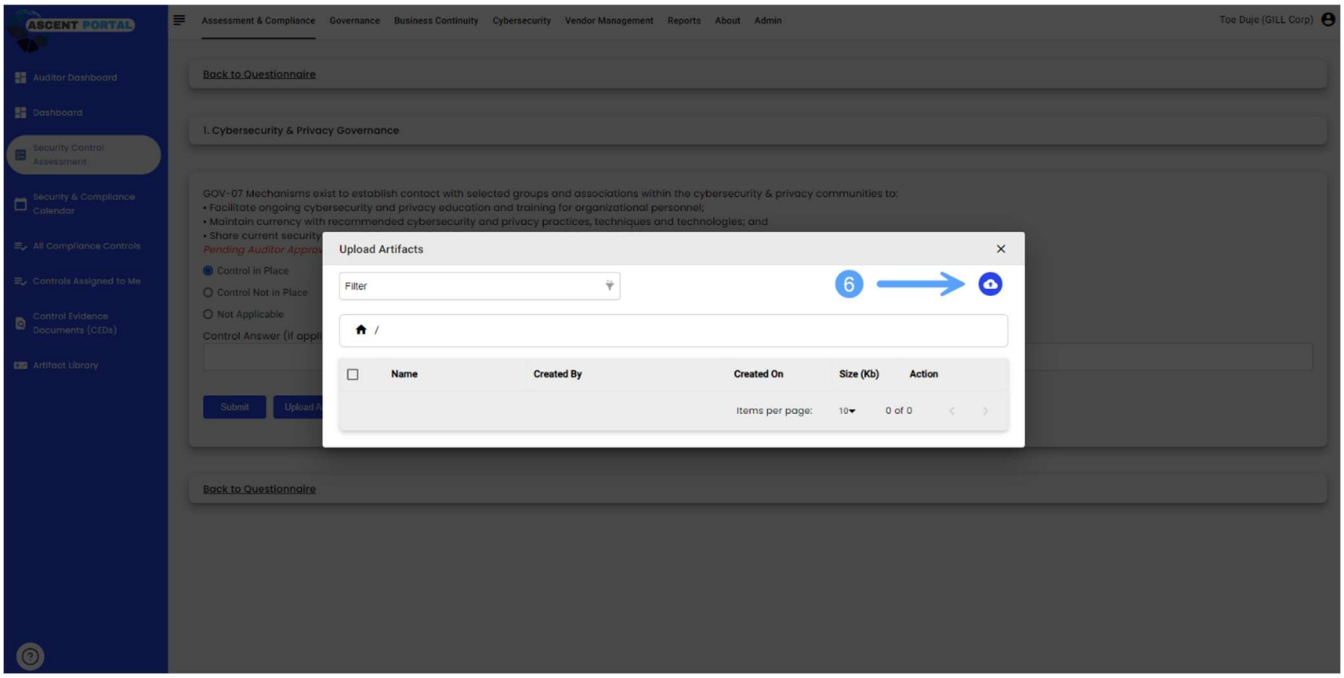
An artifact refers to a document, file, record, or any other evidence that demonstrates the implementation and effectiveness of security controls and measures within an organization. Artifacts are used to provide proof of compliance with specific security standards, policies, or regulatory requirements.

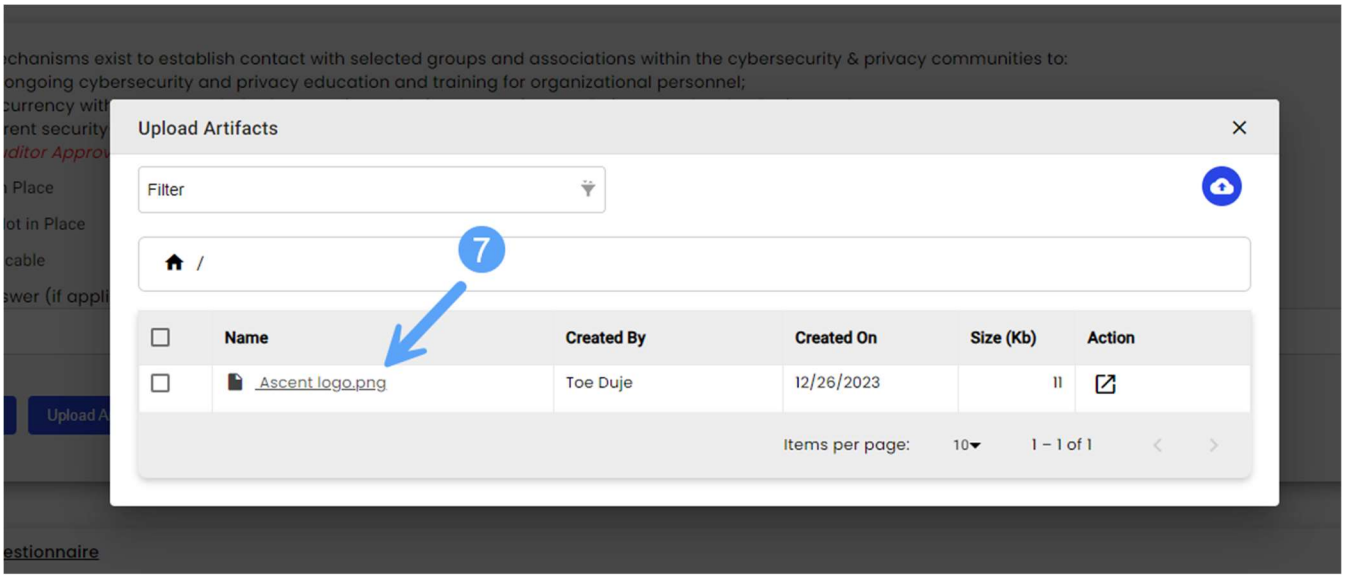
How to upload artifacts

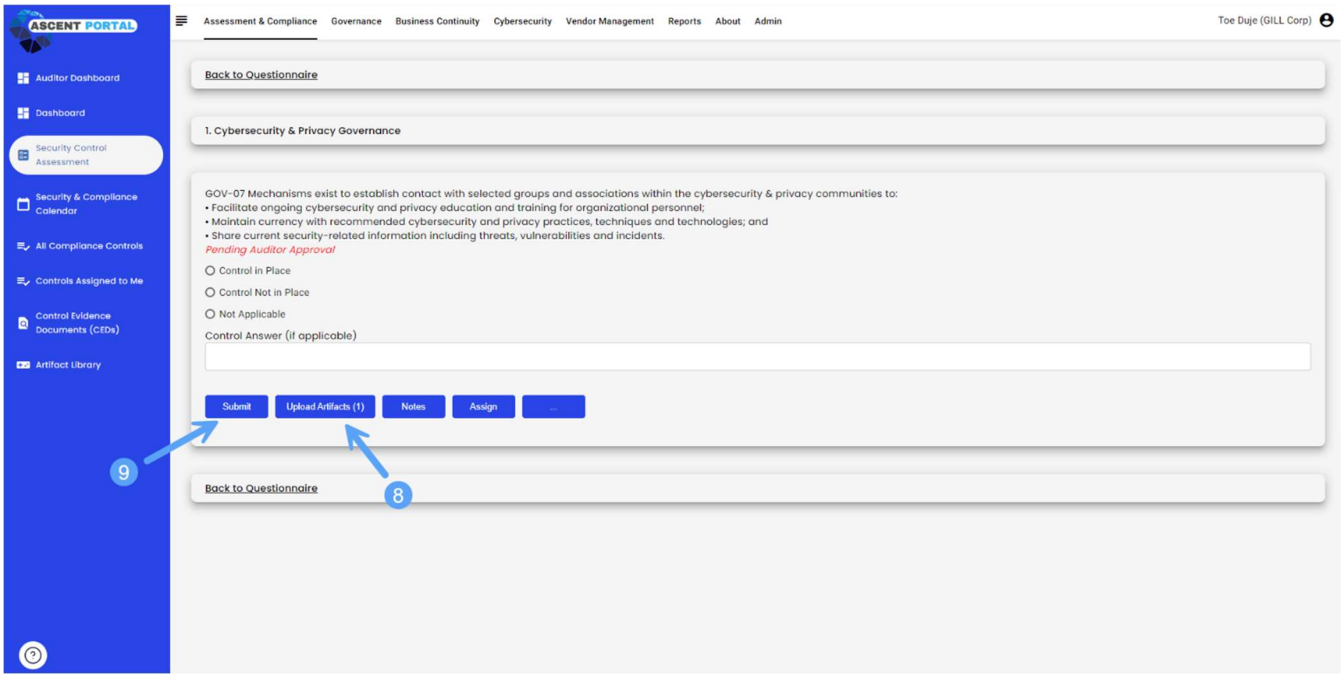
1. Click on **Assessment & Compliance (1).**
2. Click on **Security Control Assessment (2).**
3. Click the desired **Control Family Name (3).**
4. Check the appropriate status of the control (4).
5. Click **Upload Artifacts (5).**
6. Click the **blue upload button (6).** Choose the file you want to upload 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).


ASCENT PORTAL
Assessment & Compliance
Governance
Business Continuity
Cybersecurity
Vendor Management
Reports
About
Admin
Toe Duje (GILL Corp)
Auditor Dashboard
Dashboard
Security Control Assessment
Security & Compliance Calendar
All Compliance Controls
Controls Assigned to Me
Control Evidence Documents (CEDs)
Artifact Library
WISP Framework
1
2
3
Control Family Name
Score
Answered/Total
In Place
Not In Place
Not Applicable
Last Updated
1. Cybersecurity & 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
3. Cloud Security 0% 0/1 - 00% 0 0 0 12/26/2023
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
6. Cryptographic Protections 0% 0/5 - 00% 0 0 0 12/26/2023
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
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
17. Change Management 0% 0/2 - 00% 0 0 0 12/26/2023
Items per page: 50
1 – 17 of 17


ASCENT PORTAL
Assessment & Compliance
Governance
Business Continuity
Cybersecurity
Vendor Management
Reports
About
Admin
Toe Duje (GILL Corp)
Auditor Dashboard
Dashboard
Security Control Assessment
Security & Compliance Calendar
All Compliance Controls
Controls Assigned to Me
Control Evidence Documents (CEDs)
Artifact Library
Back to Questionnaire
1. Cybersecurity & Privacy Governance
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
• Share current security-related information including threats, vulnerabilities and incidents.
Pending Auditor Approval
4
Control in Place
Control Not in Place
Not Applicable
Control Answer (if applicable)
Submit
Upload Artifacts (0)
Notes
Assign
5
Back to Questionnaire

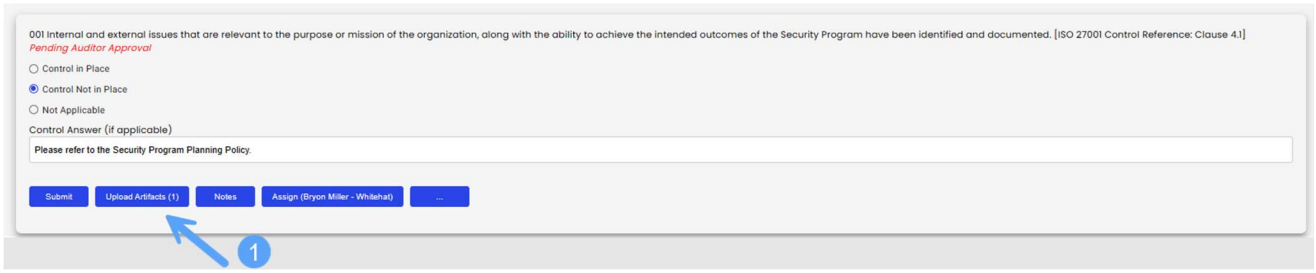

Assessment & Compliance
Governance
Business Continuity
Cybersecurity
Vendor Management
Reports
About
Admin
Back to Questionnaire
I. Cybersecurity & Privacy Governance
Upload Artifacts
Filter
6
Name
Created By
Created On
Size (Kb)
Action
Items per page:
0 of 0
Back to Questionnaire

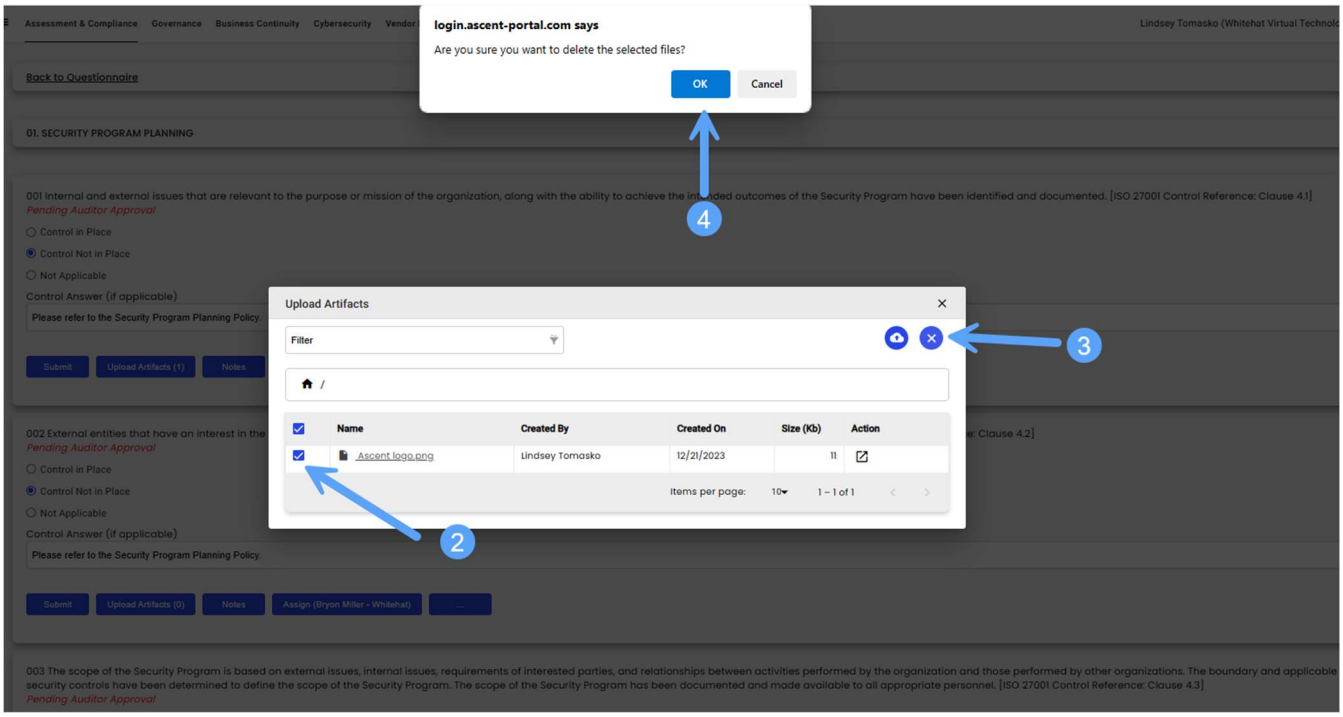

Upload Artifacts
Filter
7
Name
Created By
Created On
Size (Kb)
Action
Ascent logo.png
Toe Duje
12/26/2023
11
Items per page:
10
1 – 1 of 1



How to delete artifacts

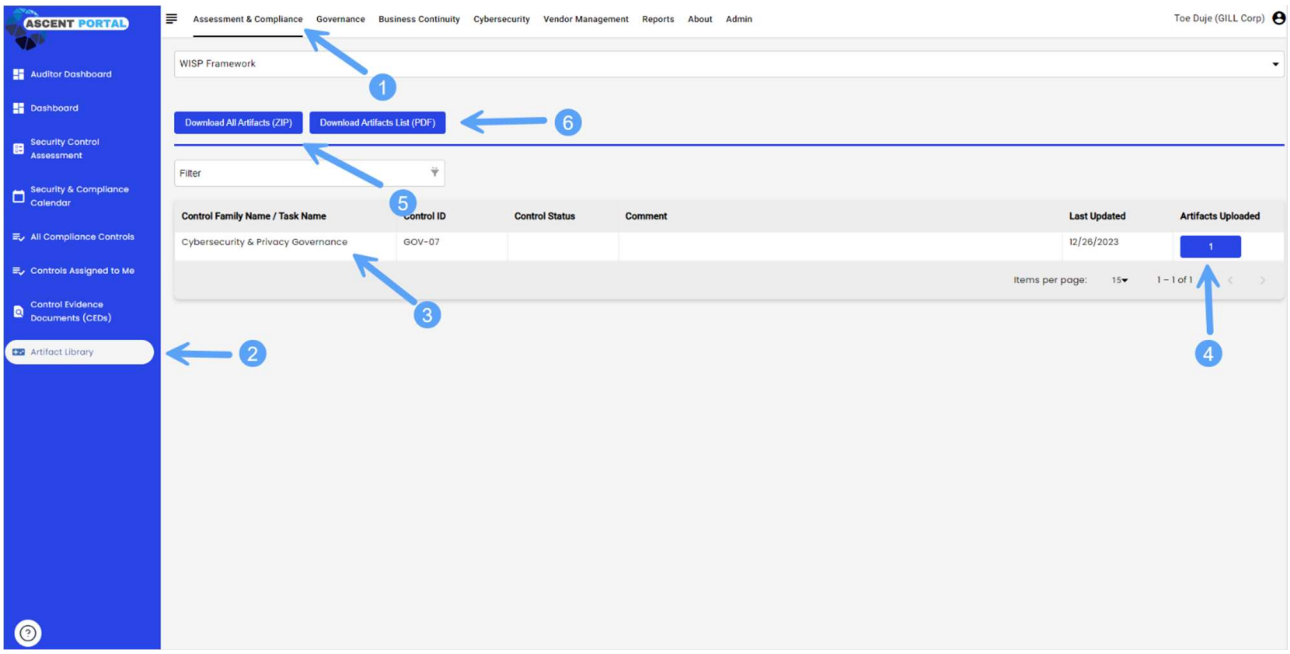
1. Click **Upload Artifacts (1).**
2. **Check the box** next to the artifact you want to delete (2).
3. Click the **X** (3).
4. Click **OK** in the pop-up menu (4).





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).



Reports

Automated Weekly Status Reports

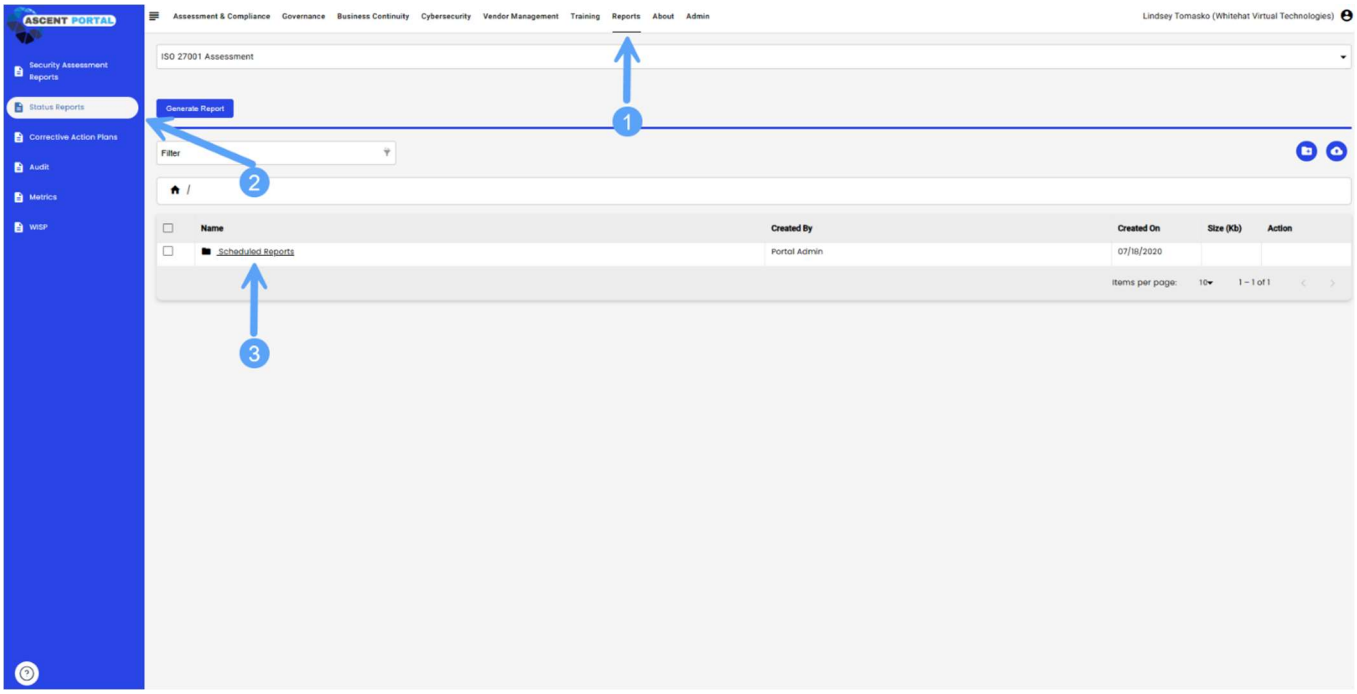
Status Reports provide a real-time status of every control contained in the selected control framework. Status Reports are automatically generated by ASCENT Portal every week and stored in the Reports tab.

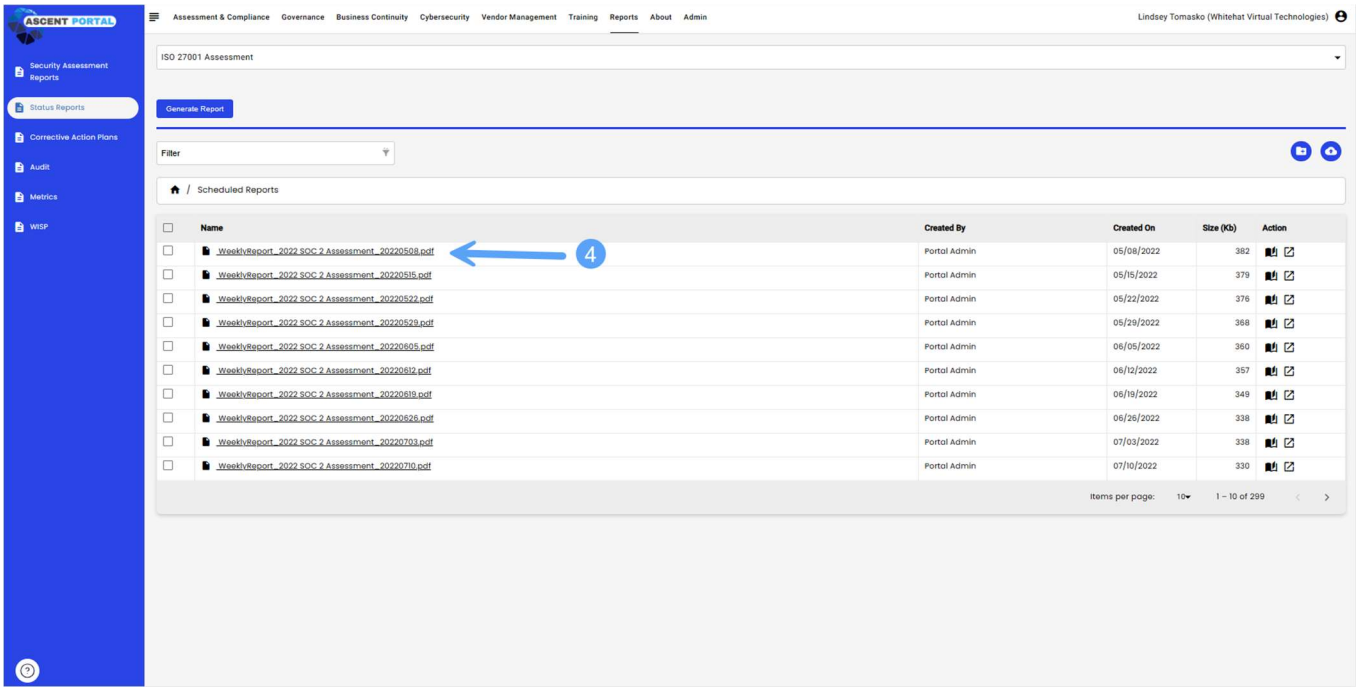
These reports contain the following graphical representations:

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

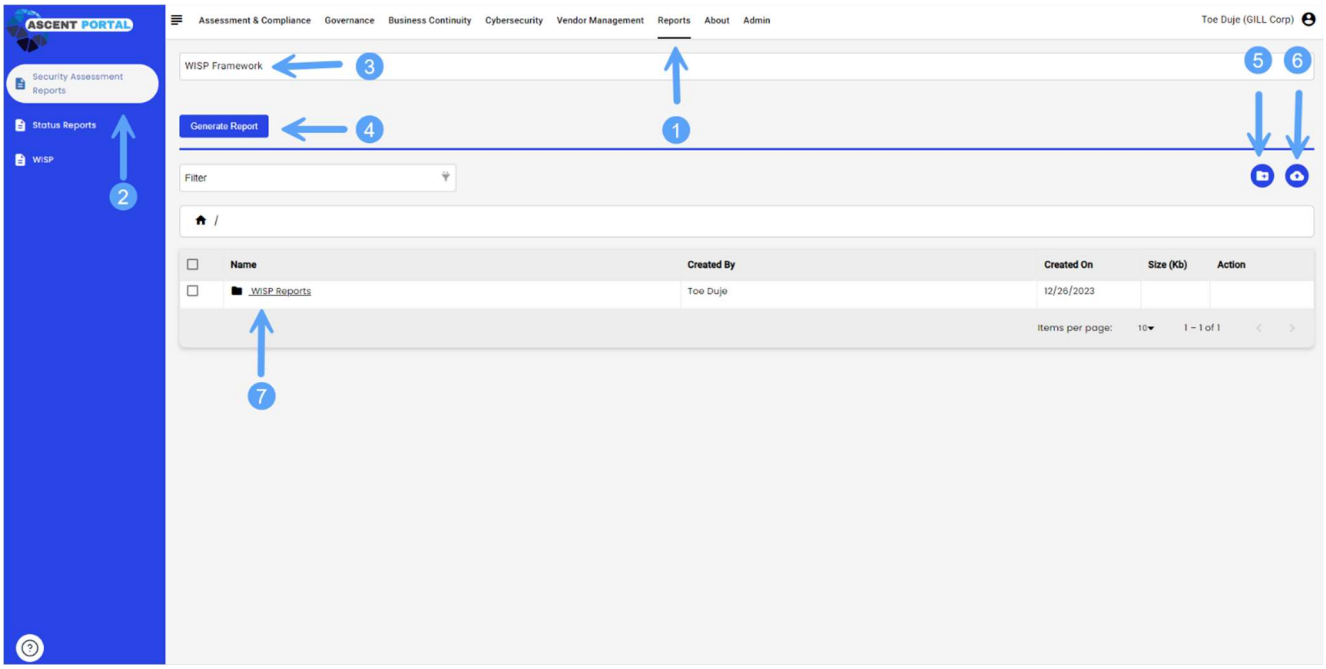
1. Click **Reports (1)**
2. Click **Status Reports (2)**
3. Here you will see the Scheduled Reports folder, which is where the auto-generated reports will be kept. (3)
4. Click the folder's name to see a list of all the reports in that folder (4).





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
Vendor Management
Reports
About
Admin
Toe Duje (GILL Corp)
Security Assessment Reports
Status Reports
WISP
WISP Framework
Generate Report
Filter
Name
Created By
Created On
Size (Kb)
Action
WISP Reports
Toe Duje
12/26/2023
Items per page:
10
1 – 1 of 1
1
2
3
4
5
6
7

Chapter 3: Using the Portal

General Portal

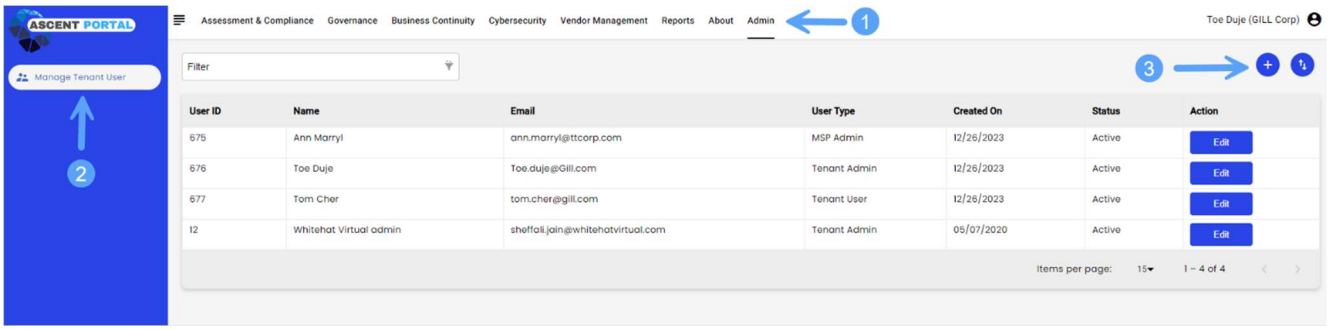
Types of Access

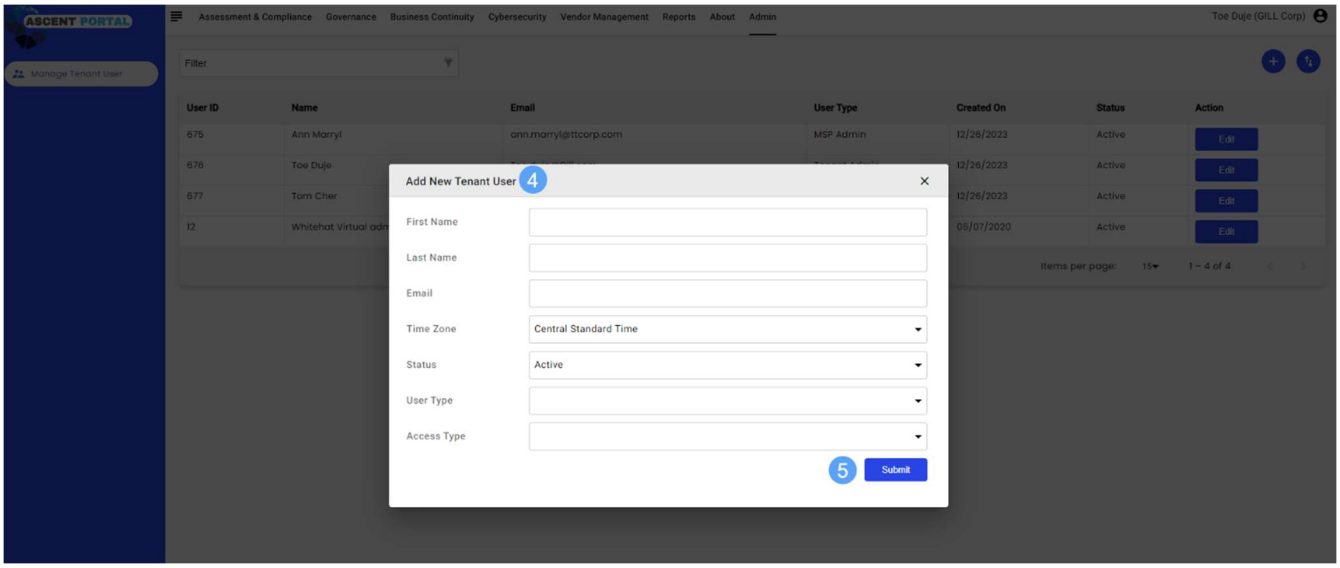
Below are the types of access and what each type has access to.

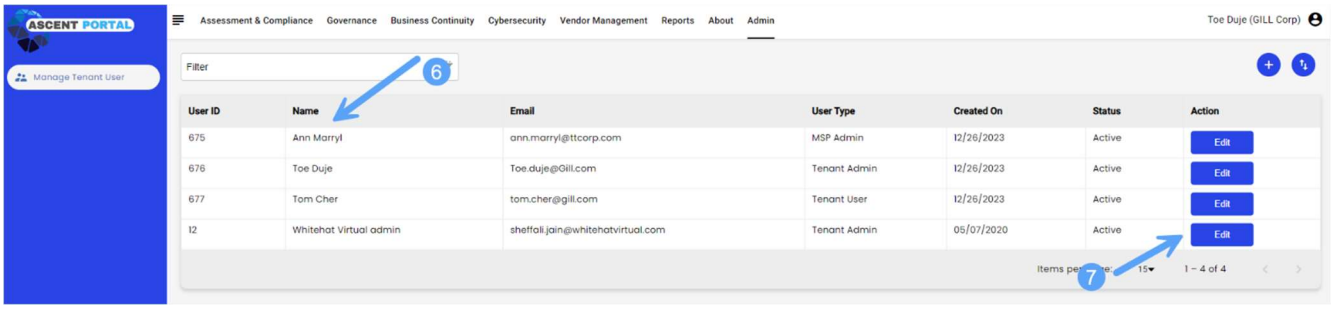
Modules	Sections	MSP	Tenant Admin	Tenant Users
Assessment & Compliance	MSP Dashboard	X		
Assessment & Compliance	Admin Dashboard		X	
Assessment & Compliance	Dashboard	X	X	X
Assessment & Compliance	Security Control Assessment	X	X	X
Assessment & Compliance	Security Compliance Calendar	X	X	X
Assessment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





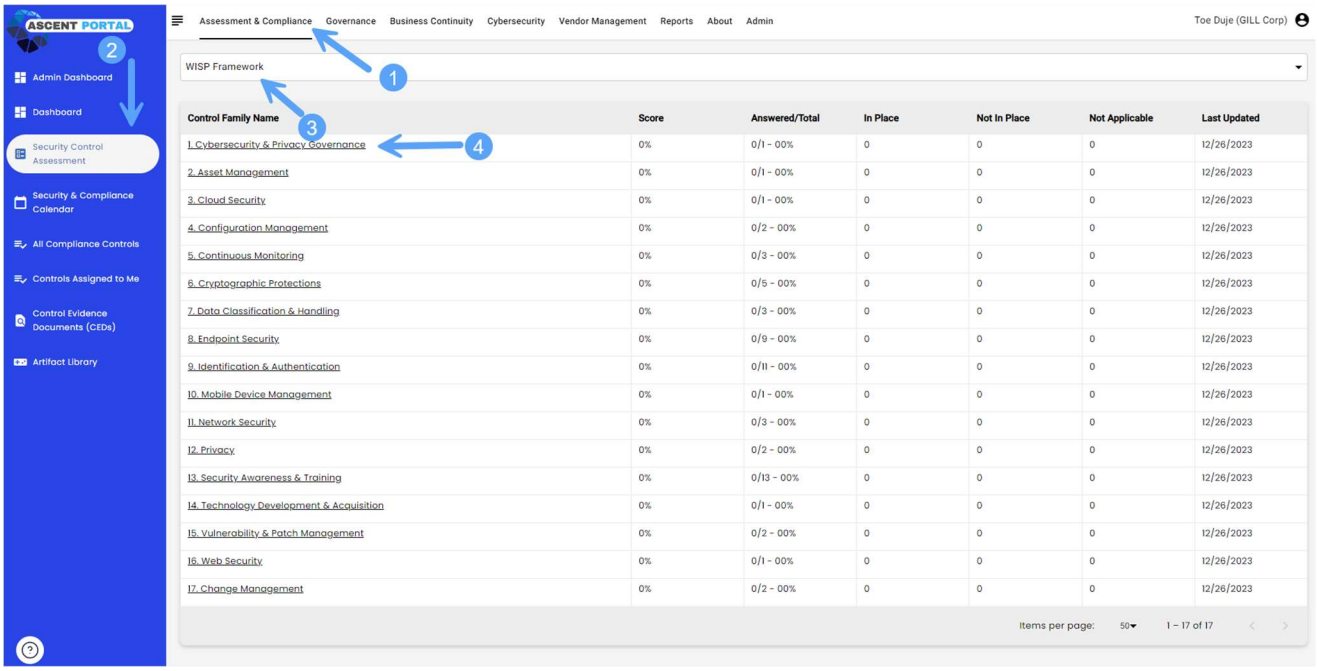


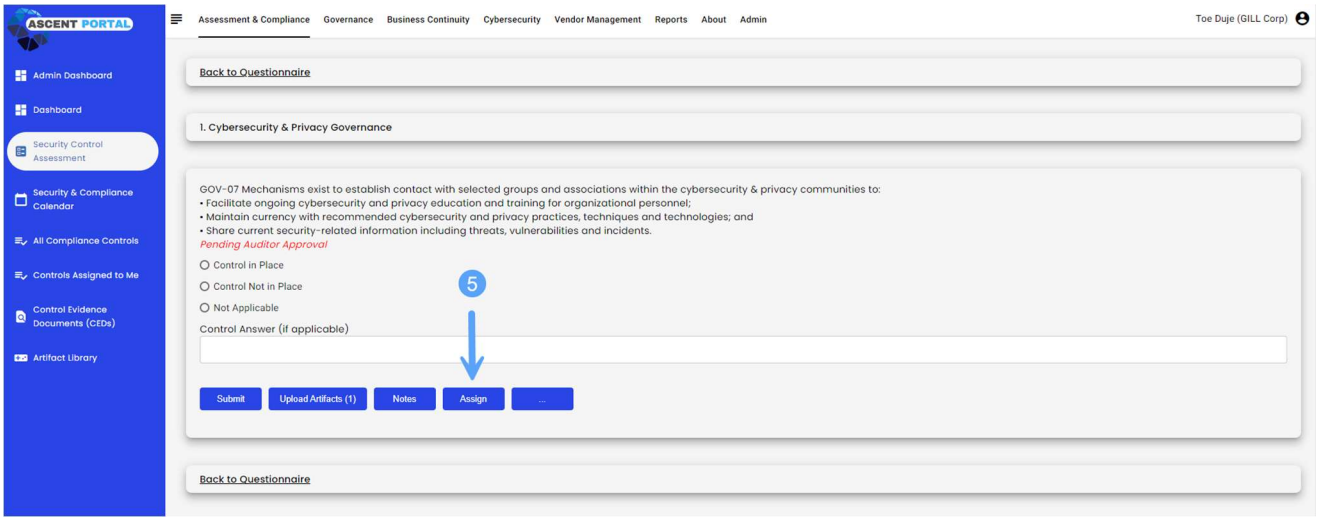
Assigning and Managing Controls

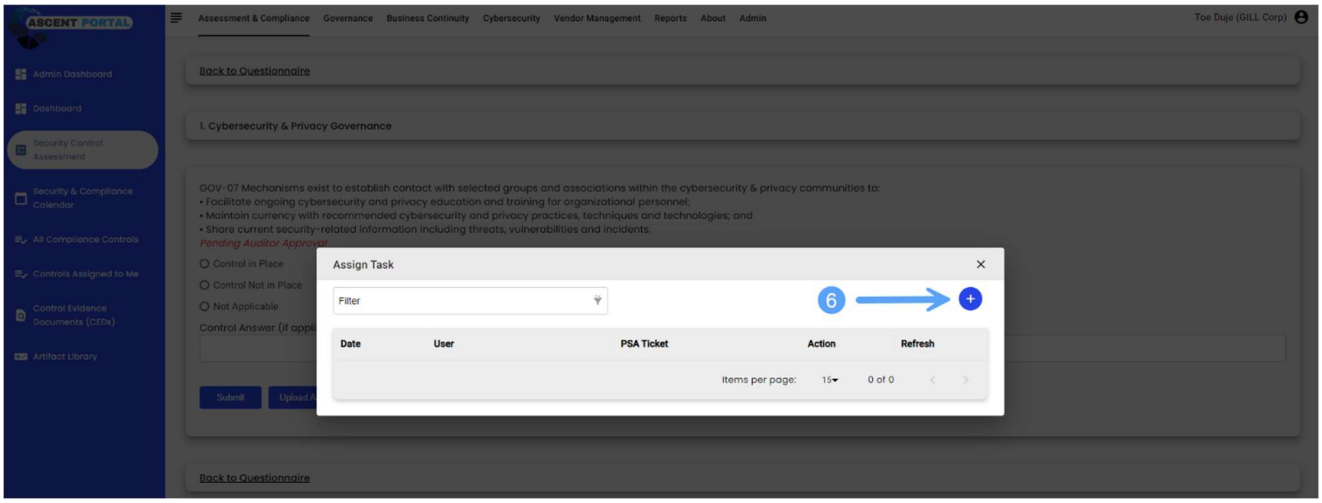
All controls must be assigned to an owner and be given a due date. The owner is responsible for ensuring the control is kept in compliance and will be made automatically via email once the control is assigned to them.

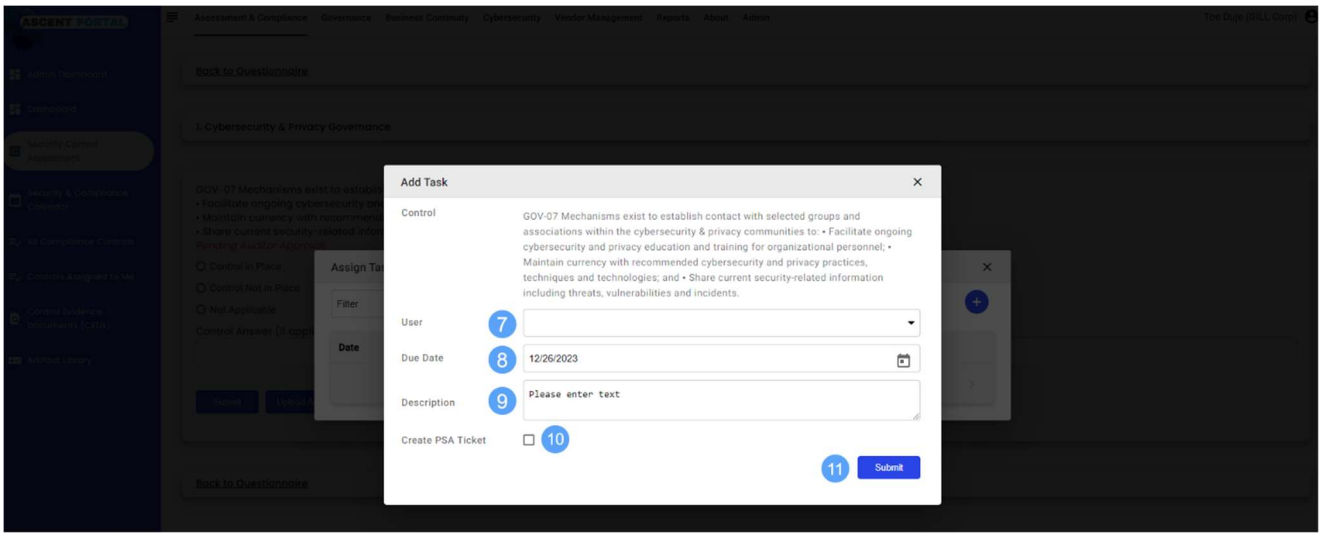
To assign a control:

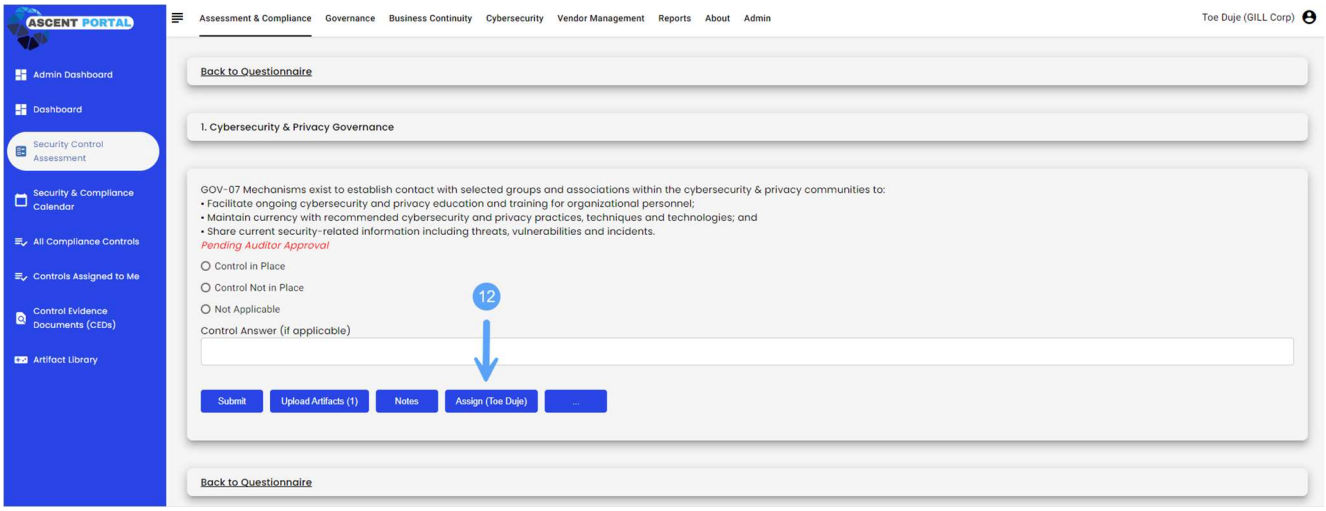
1. Click **Assessment & Compliance** (1)
2. Click **Security Control Assessment** (2)
3. Click on the desired Framework via the drop-down menu (3)
4. Click on the desired **Control Family Name** (4)
5. In the desired control, click **Assign** (5)
6. In the popup box, click the **plus sign** (6)
7. Click 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)


ASCENT PORTAL
Assessment & Compliance
Governance
Business Continuity
Cybersecurity
Vendor Management
Reports
About
Admin
Toe Duje (GILL Corp)
Admin Dashboard
Dashboard
Security Control Assessment
Security & Compliance Calendar
All Compliance Controls
Controls Assigned to Me
Control Evidence Documents (CEDs)
Artifact Library
WISP Framework
1
2
3
4
Control Family Name
Score
Answered/Total
In Place
Not In Place
Not Applicable
Last Updated
1. Cybersecurity & 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
3. Cloud Security 0% 0/1 - 00% 0 0 0 12/26/2023
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
6. Cryptographic Protections 0% 0/5 - 00% 0 0 0 12/26/2023
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
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
17. Change Management 0% 0/2 - 00% 0 0 0 12/26/2023
Items per page: 50
1 – 17 of 17


ASCENT PORTAL
Assessment & Compliance
Governance
Business Continuity
Cybersecurity
Vendor Management
Reports
About
Admin
Toe Duje (GILL Corp)
Admin Dashboard
Dashboard
Security Control Assessment
Security & Compliance Calendar
All Compliance Controls
Controls Assigned to Me
Control Evidence Documents (CEDs)
Artifact Library
Back to Questionnaire
1. Cybersecurity & Privacy Governance
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
• Share current security-related information including threats, vulnerabilities and incidents.
Pending Auditor Approval
Control in Place
Control Not in Place
Not Applicable
Control Answer (if applicable)
5
Submit
Upload Artifacts (1)
Notes
Assign
...
Back to Questionnaire

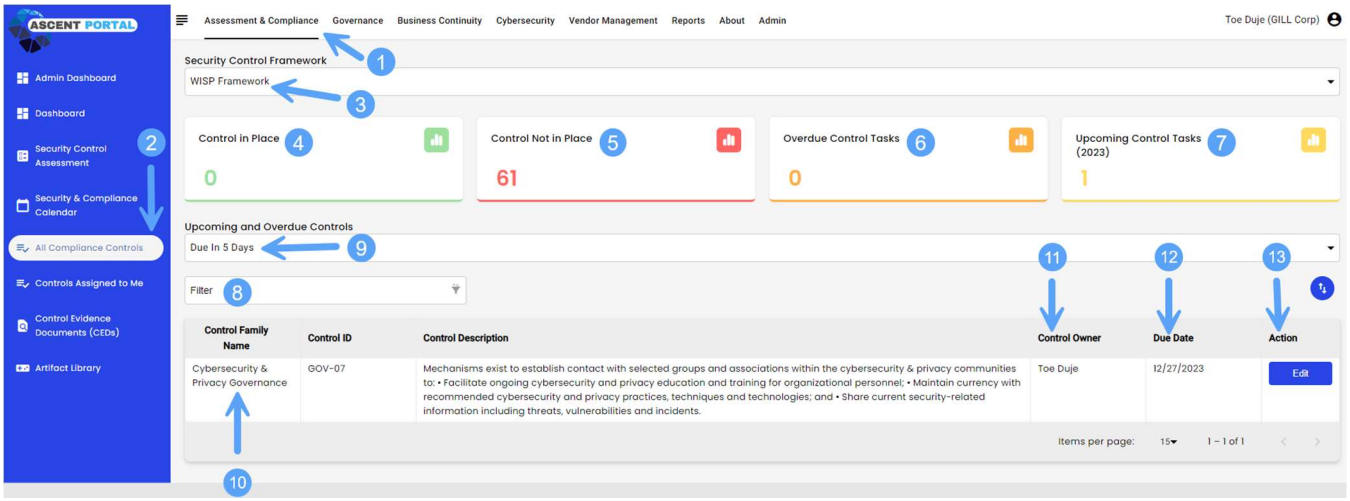

ASCENT PORTAL
Assessment & Compliance
Governance
Business Continuity
Cybersecurity
Vendor Management
Reports
About
Admin
Toe Duje (GILL Corp)
Admin Dashboard
Dashboard
Security Control Assessment
Security & Compliance Calendar
All Compliance Controls
Controls Assigned to Me
Control Evidence Documents (CEDs)
Artifact Library
Back to Questionnaire
1. Cybersecurity & Privacy Governance
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
• Share current security-related information including threats, vulnerabilities and incidents.
Pending Auditor Approval
Control in Place
Control Not in Place
Not Applicable
Control Answer (if appl
Submit
Assign Task
Filter
6
Date
User
PSA Ticket
Action
Refresh
Items per page:
15
0 of 0
Back to Questionnaire


Add Task
Control
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 • Share current security-related information including threats, vulnerabilities and incidents.
User
7
Due Date
8
12/26/2023
Description
9
Please enter text
Create PSA Ticket
10
11
Submit


ASCENT PORTAL
Assessment & Compliance
Governance
Business Continuity
Cybersecurity
Vendor Management
Reports
About
Admin
Toe Duje (GILL Corp)
Admin Dashboard
Dashboard
Security Control Assessment
Security & Compliance Calendar
All Compliance Controls
Controls Assigned to Me
Control Evidence Documents (CEDs)
Artifact Library
Back to Questionnaire
1. Cybersecurity & Privacy Governance
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
• Share current security-related information including threats, vulnerabilities and incidents.
Pending Auditor Approval
Control in Place
Control Not in Place
Not Applicable
12
Control Answer (if applicable)
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).



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*

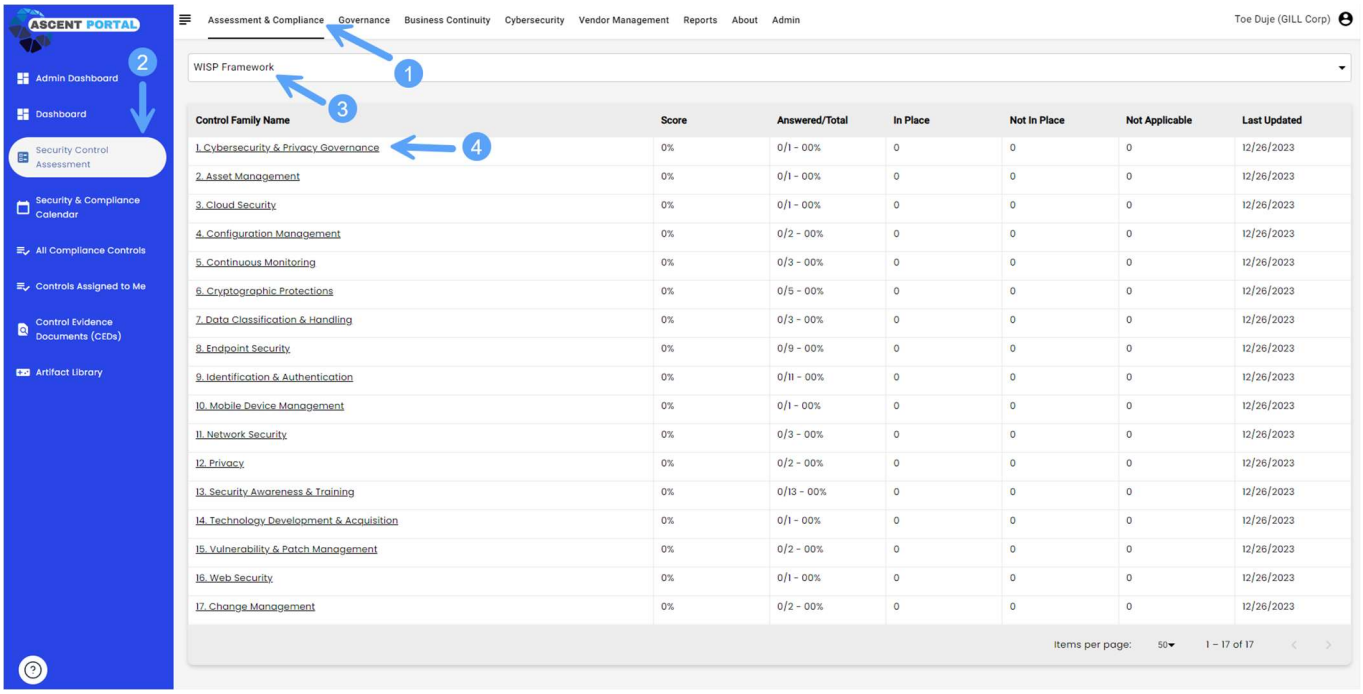
1. The control does not apply to the organization

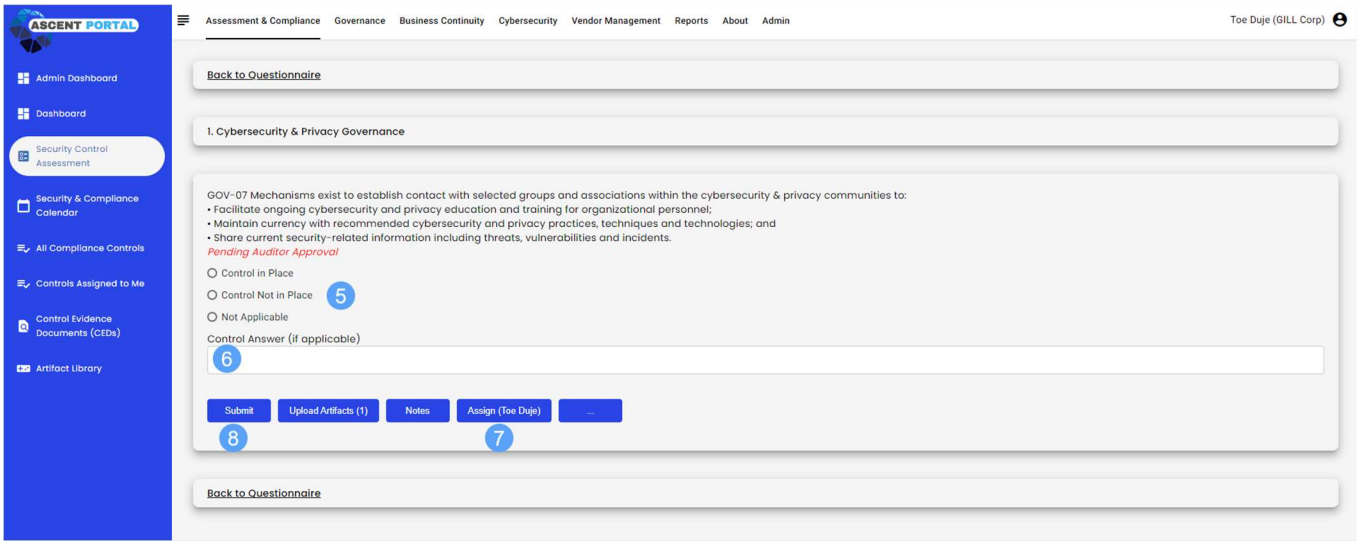
f. Provide the comments/answers as applicable under **Control Answer** (6)

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)



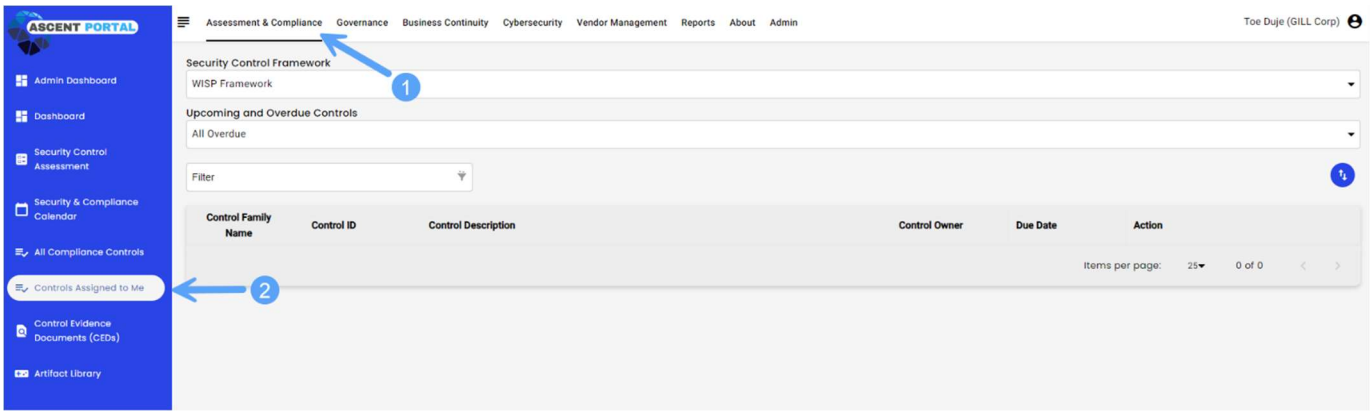


2. *Option #2*

a. Click **Assessment & Compliance** (1)

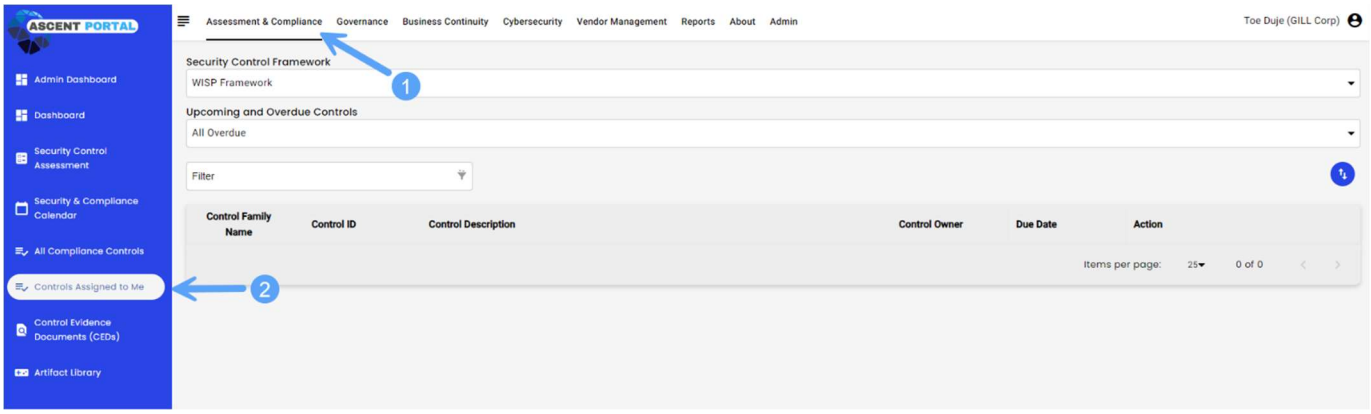
b. Click **Controls Assigned to Me** (2)

c. Here you will see a list of controls assigned to you, which you can act on.



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.



Alerts to Help Manage Controls:

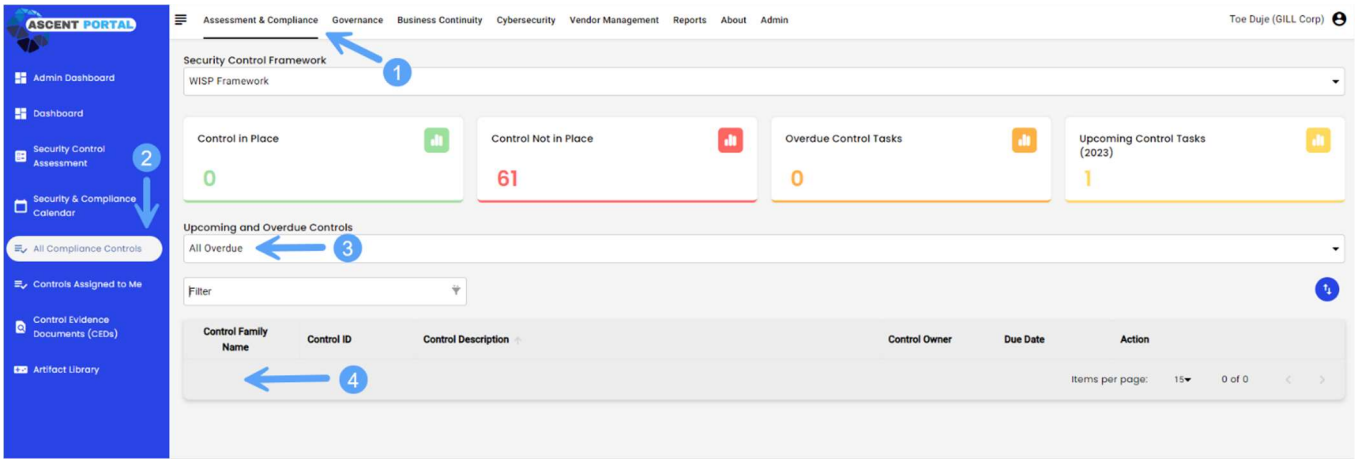
The automated alerts will help users stay on top of the tasks assigned to them, with several reminders along the way.

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:

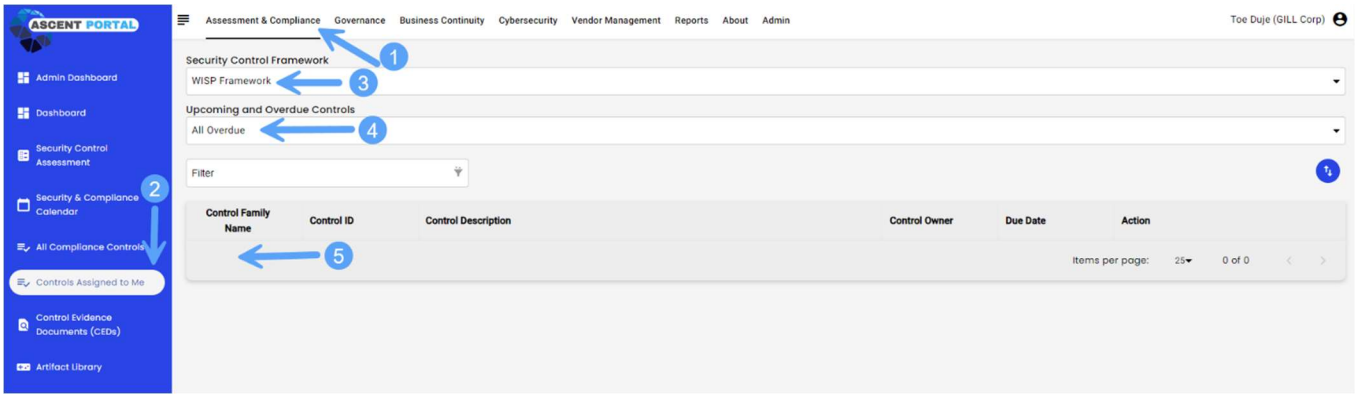
1. Click **Assessment & Compliance** (1)
2. Click **All Compliance Controls** (2)
3. Click the drop-down to see **Upcoming and Overdue Controls** (3). This drop-down will show you controls that are:
    a. Overdue
    b. Due in 3 days
    c. Due in 5 days
    d. All tasks
4. The list will appear below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



Viewing and Managing Your to do List of Controls

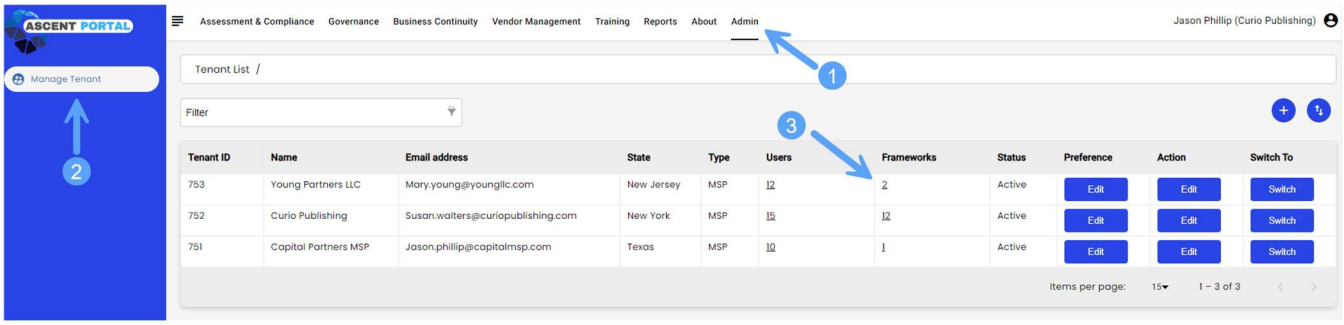
To plan out your personal workload, you can view your upcoming controls to help you stay on top of your to-do list.

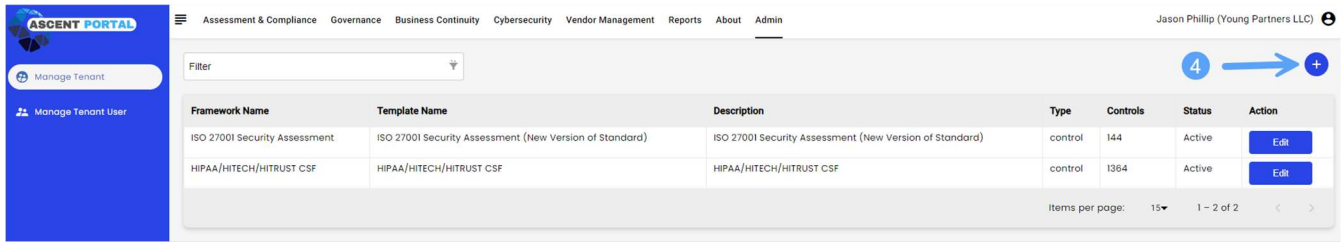
1. Click **Assessment & Compliance** (1)
2. Click **Controls Assigned to Me** (2)
3. Choose the framework from the drop-down menu (3)
4. Choose the filter you would like to view (4)
    a. This drop-down will show you controls that are:
        i. Overdue
        ii. Due in 3 days
        iii. Due in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

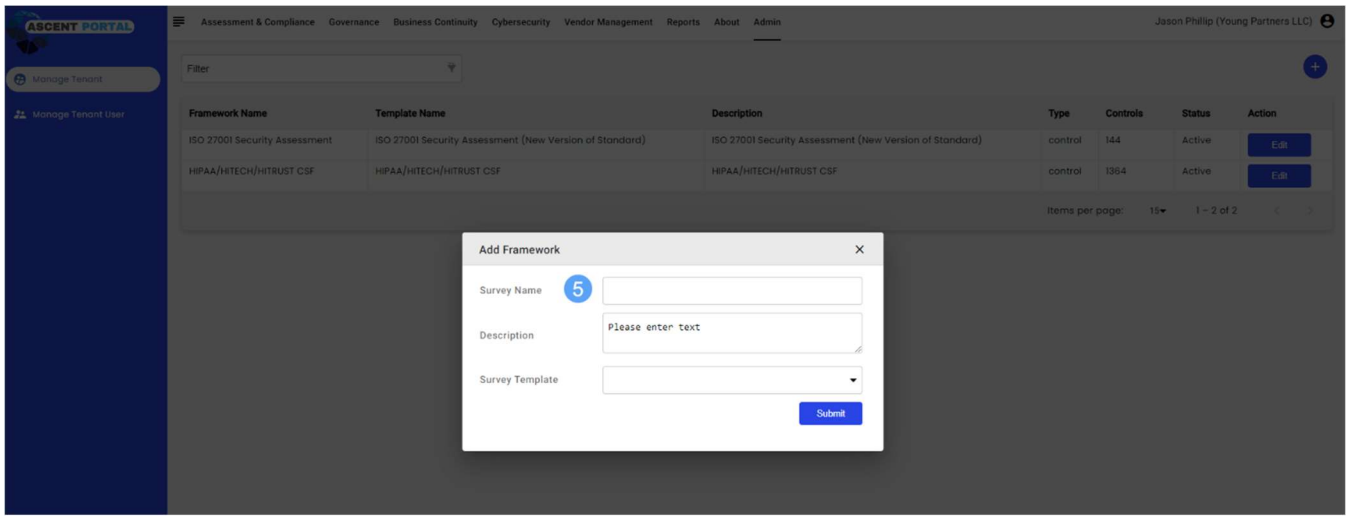


Assigning Frameworks

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.
4. 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)







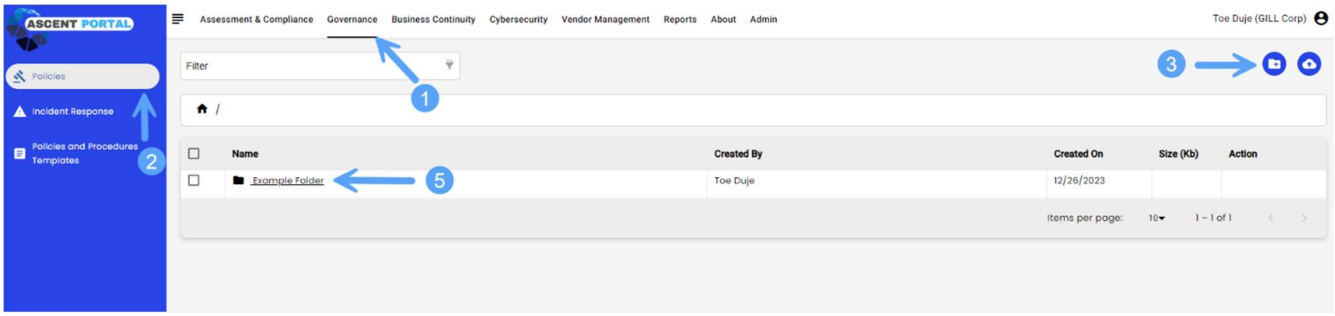
Governance

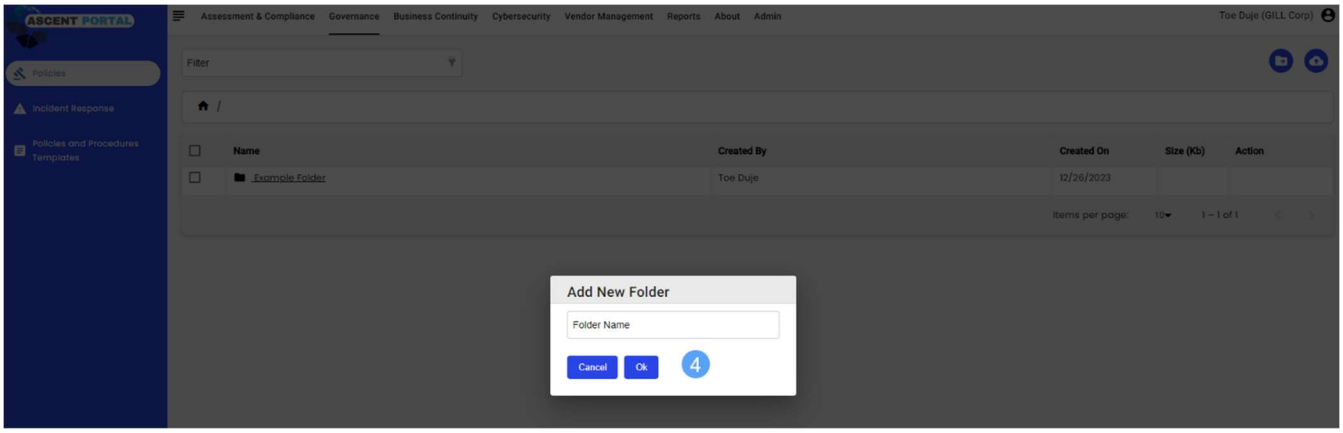
Security Policies are the foundation of any organized, efficient Security Program. They dictate the control requirements for the organization.

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**

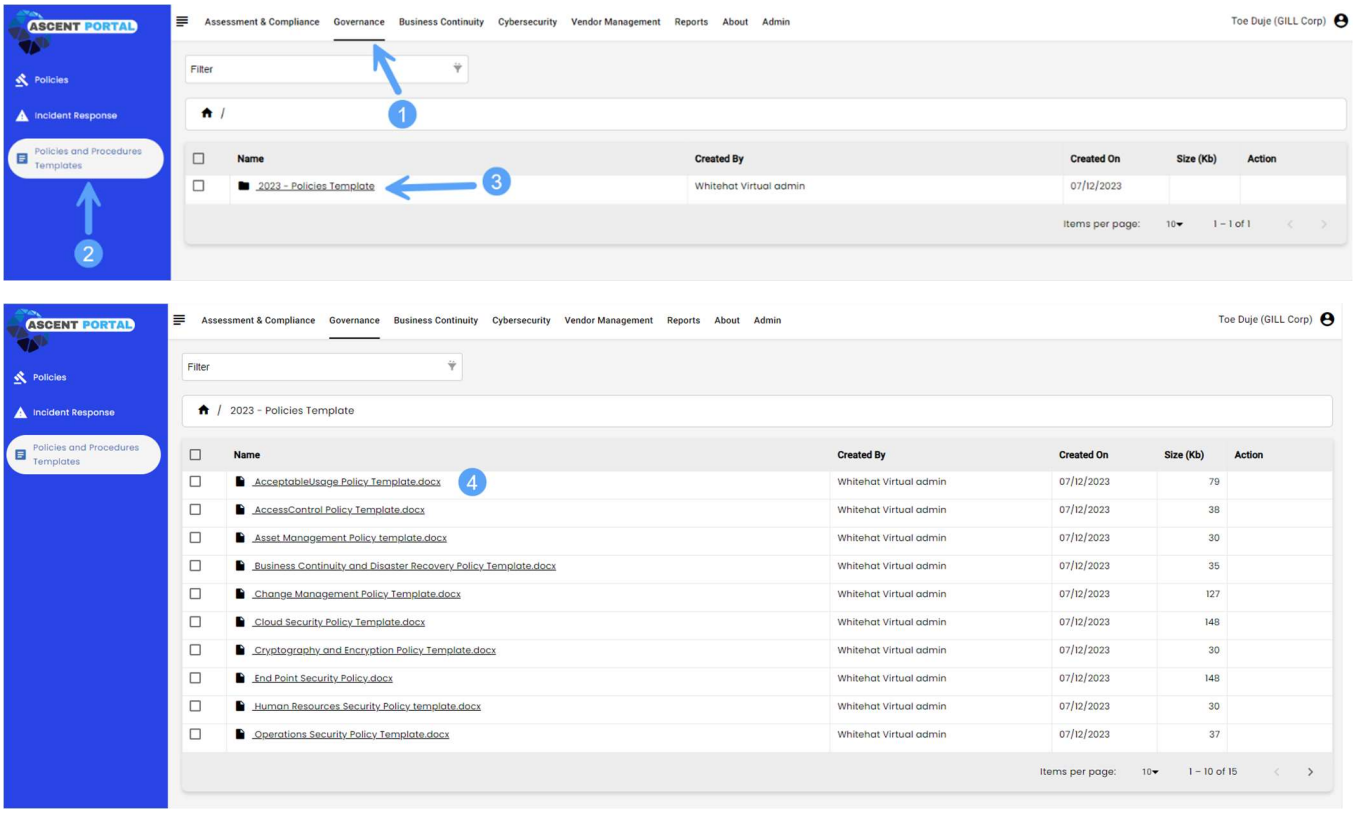




Templates

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).



Incident Response

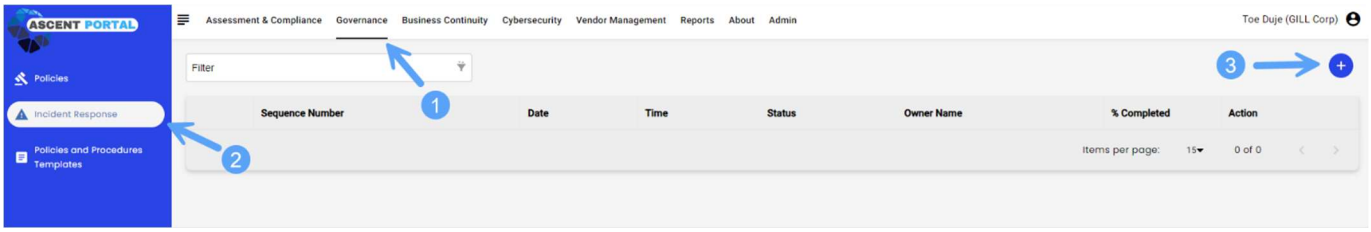
It is imperative to follow a detailed, prescribed process when navigating a security incident. By using the tools within the Portal, you and your team will be guided through the entire process from start to finish.

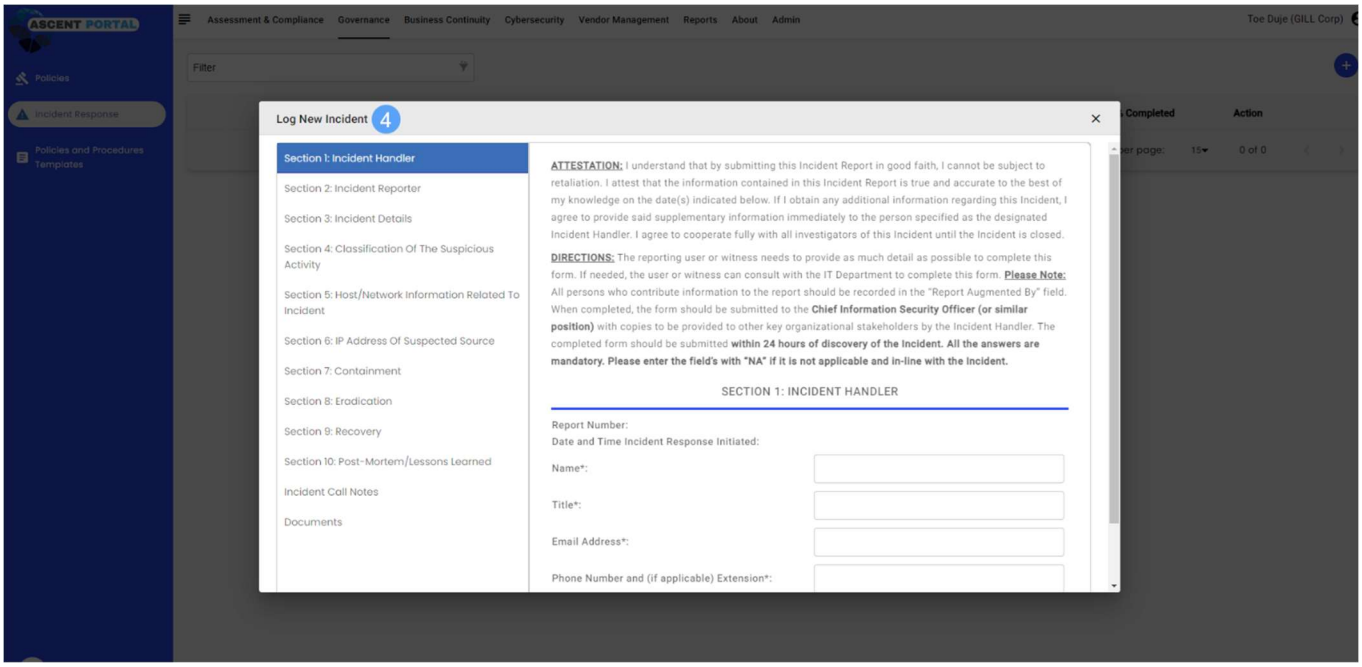
Incident Response Management

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
Assessment & Compliance
Governance
Business Continuity
Cybersecurity
Vendor Management
Reports
About
Admin
Toe Duje (GILL Corp)
Policies
Incident Response
Policies and Procedures Templates
Filter
1
2
3
Sequence Number
Date
Time
Status
Owner Name
% Completed
Action
Items per page:
15
0 of 0


Log New Incident
4
Section 1: 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 9: 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 retaliation. 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 until the Incident is closed.
DIRECTIONS: The reporting user or witness needs to provide as much detail as possible to complete this form. If needed, the user or witness can consult with the IT Department to complete this form. Please Note: All persons who contribute information to the report should be recorded in the "Report Augmented By" field. When completed, the form should be submitted to the Chief Information Security Officer (or similar position) with copies to be provided to other key organizational stakeholders by the Incident Handler. The completed form should be submitted within 24 hours of discovery of the incident. All the answers are mandatory. Please enter the field's with "NA" if it is not applicable and in-line with the incident.
SECTION 1: INCIDENT HANDLER
Report Number:
Date and Time Incident Response Initiated:
Name*:
Title*:
Email Address*:
Phone Number and (if applicable) Extension*:

Chapter 4: Using the Portal

MSP

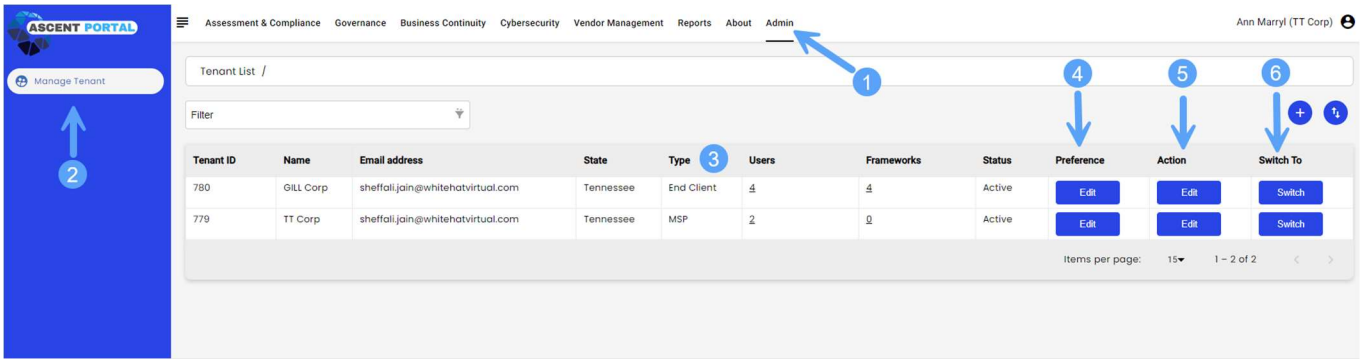
Navigating the admin section

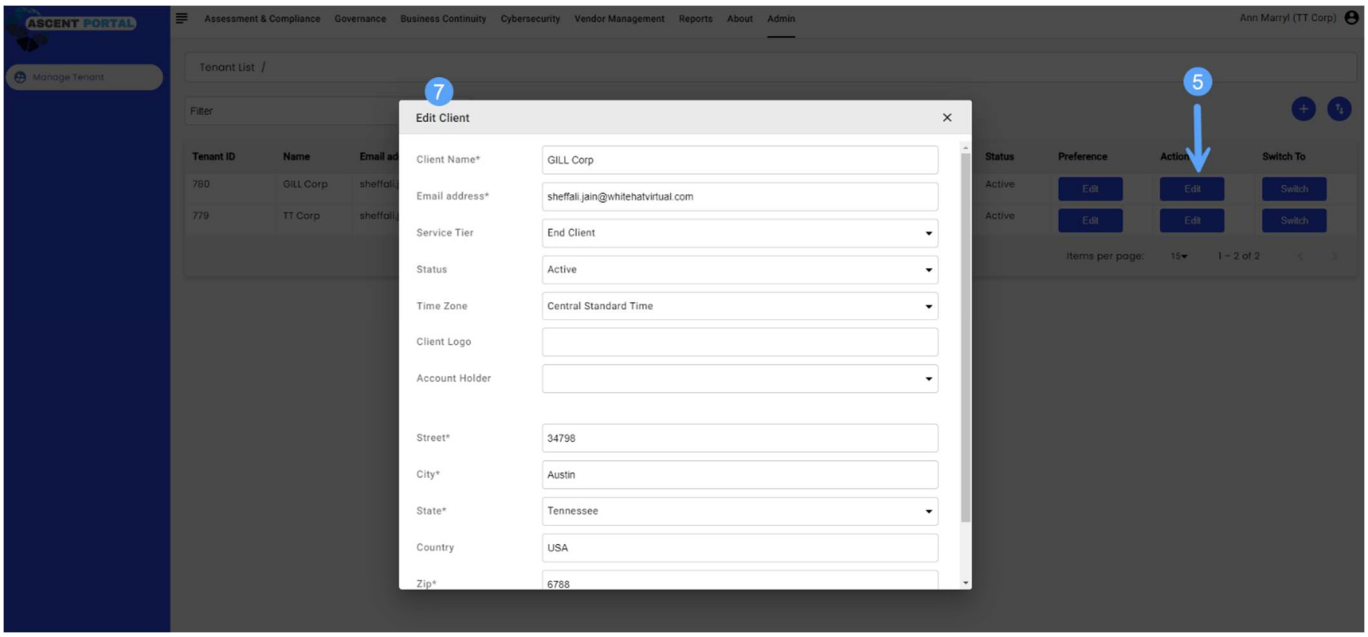
Within the **Admin tab** (1), you will be able to manage your own Portal for your MSP organization, as well as the customers, or tenants, that reside within the Portal under your organization.

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.

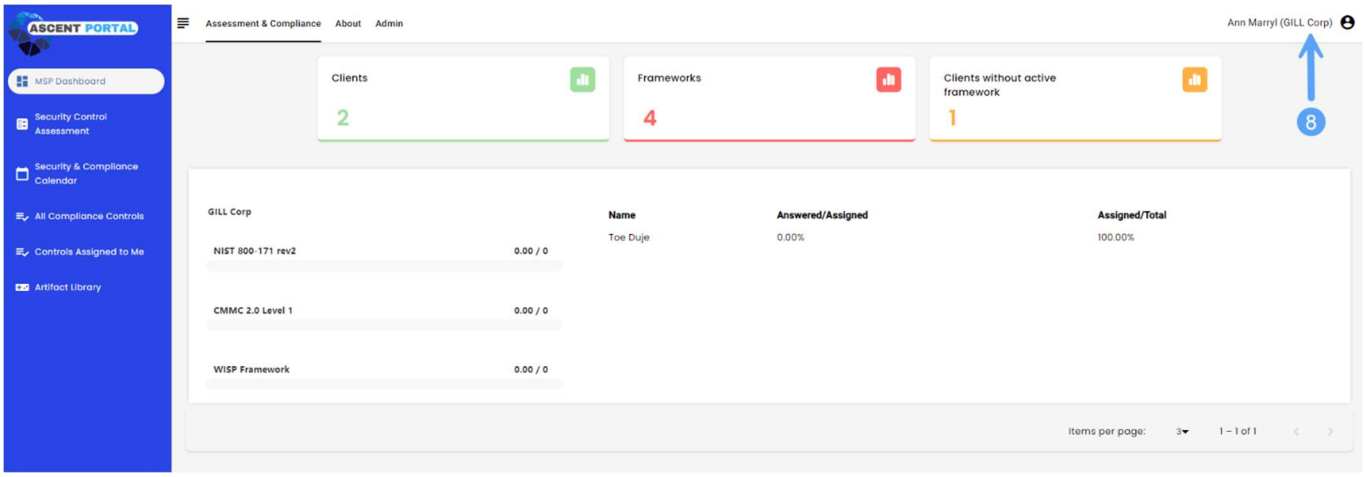
Under **Action** (5), you can edit the customer information (7).



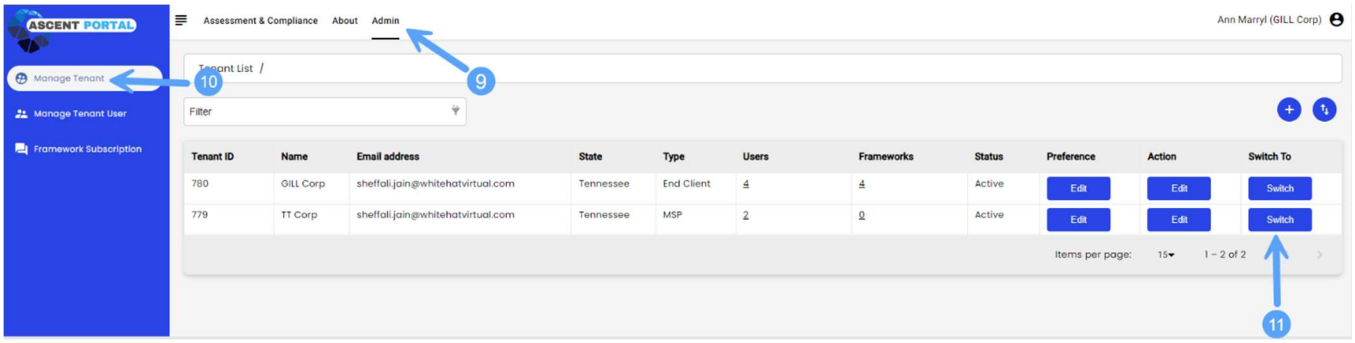


By clicking **Switch** (6), you will switch to seeing that customer's Portal. This is especially helpful once you have many tenants under your own.

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).



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.



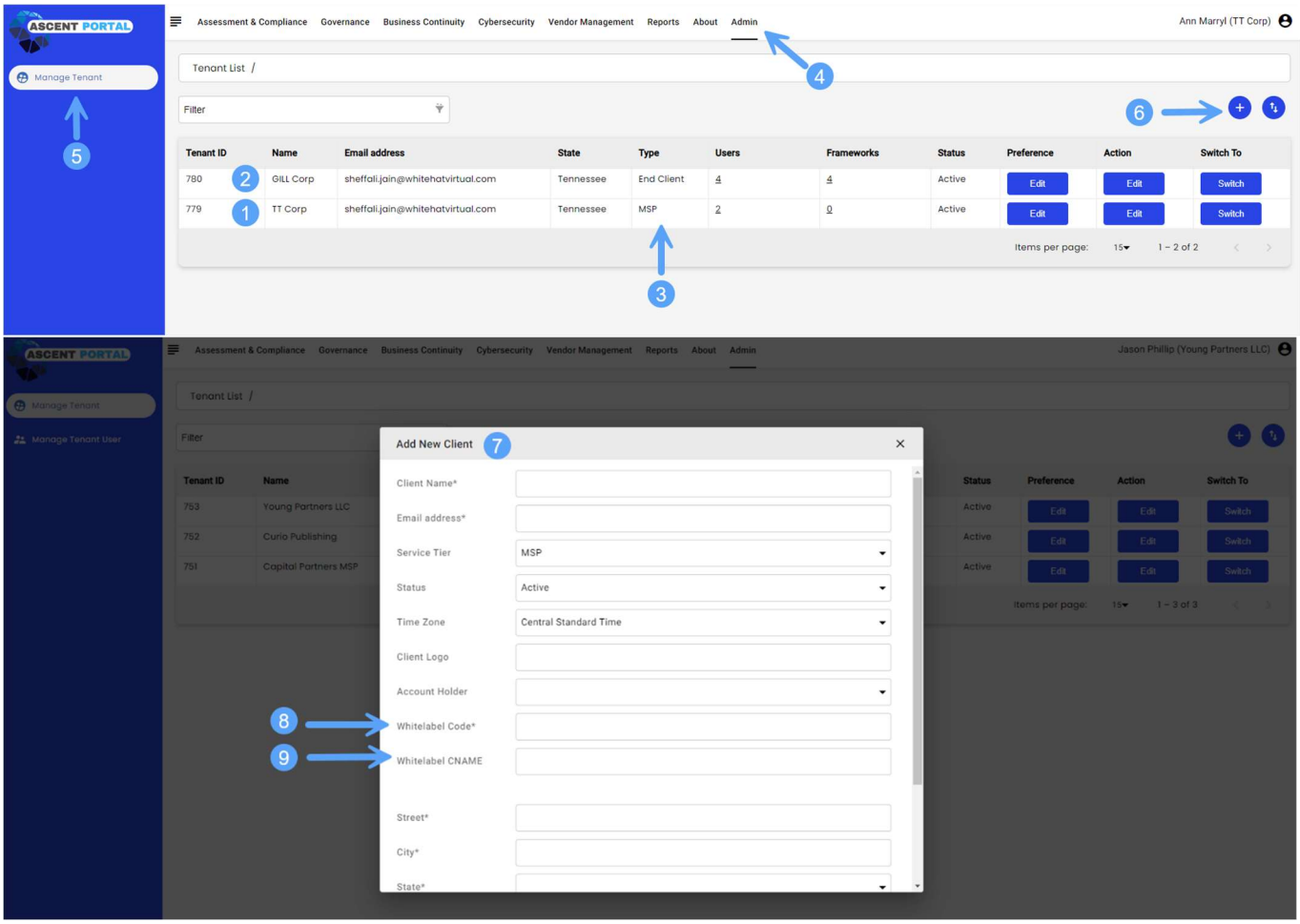
Upon signing in as the MSP admin, you will see a tenant for your own organization. In this example, it is TT Corp (1).

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).

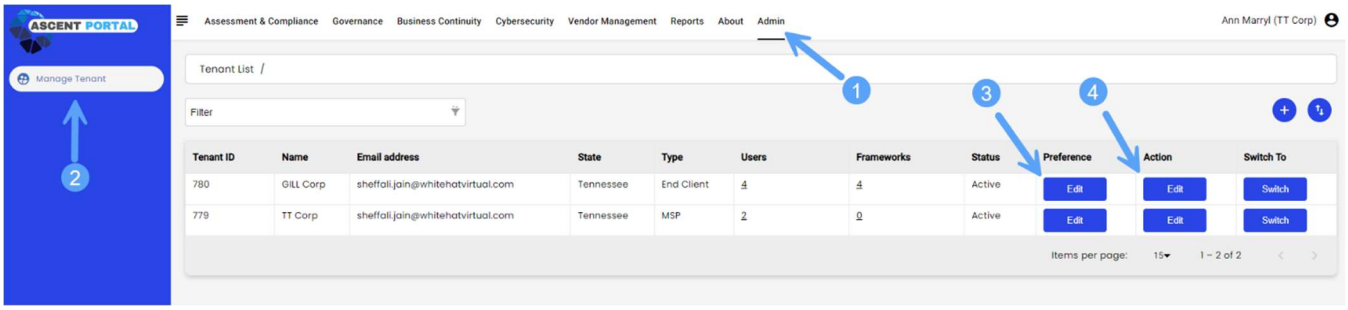
1. Click **Admin** (4)
2. Click **Manage Tenant** (5)
3. Click the **plus sign** (6)

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



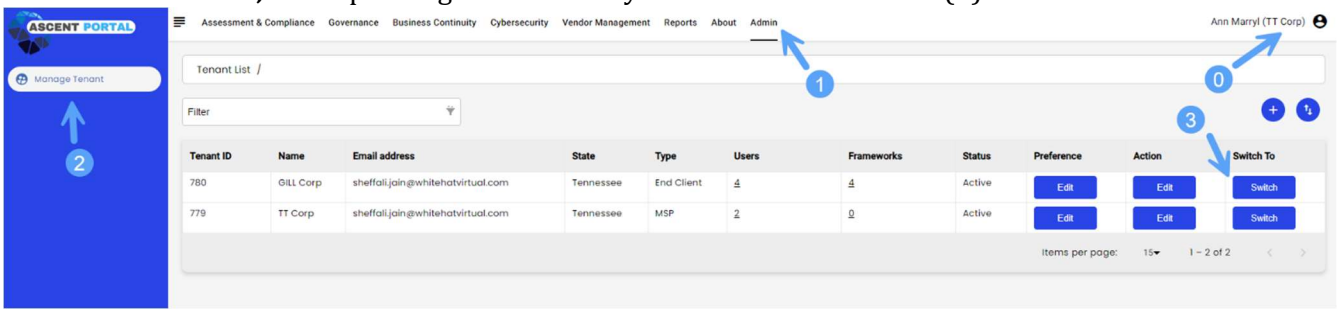
How to edit tenant details

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.**

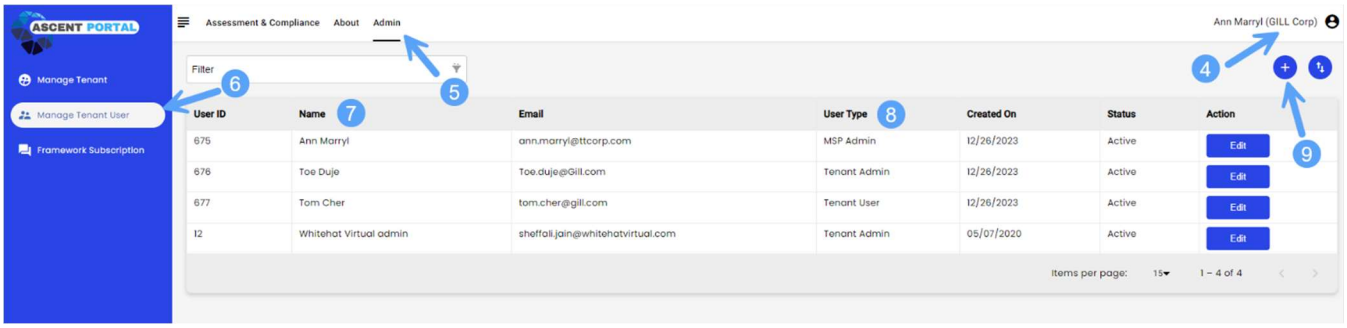


How to add users to a tenant

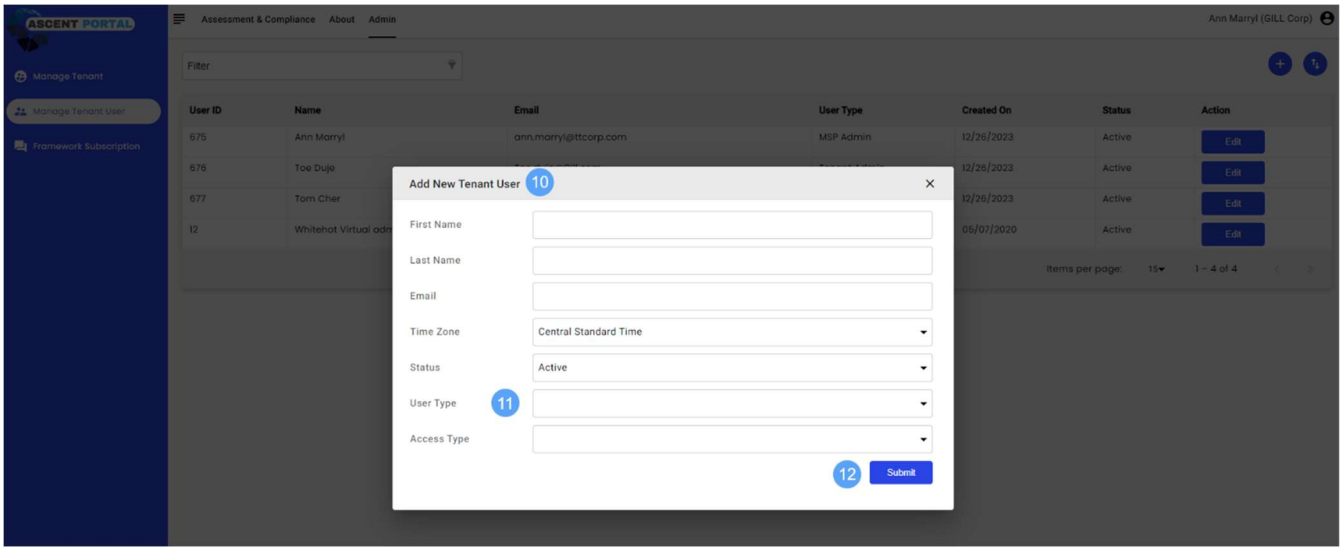
1. Log in to the Portal, which will log you in as the admin for your MSP organization (confirmed by the top right corner, which will state which organization you are logged in as) (0).
2. Click **Admin** (1).
3. Click **Manage Tenant** (2).
4. Click **Switch,** corresponding to the tenant you need to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



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).



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

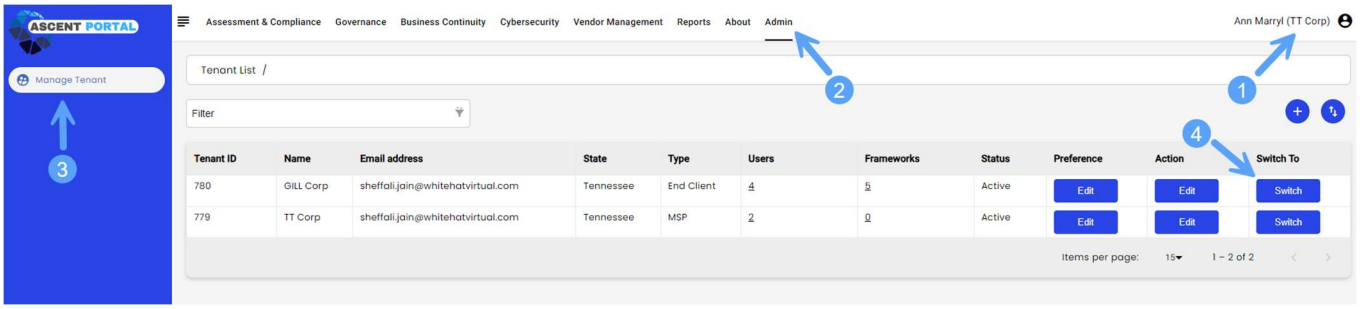


A welcome Email from the ASCENT Portal will be sent to the User with a link to set their password. The new user will need to follow the below directions:

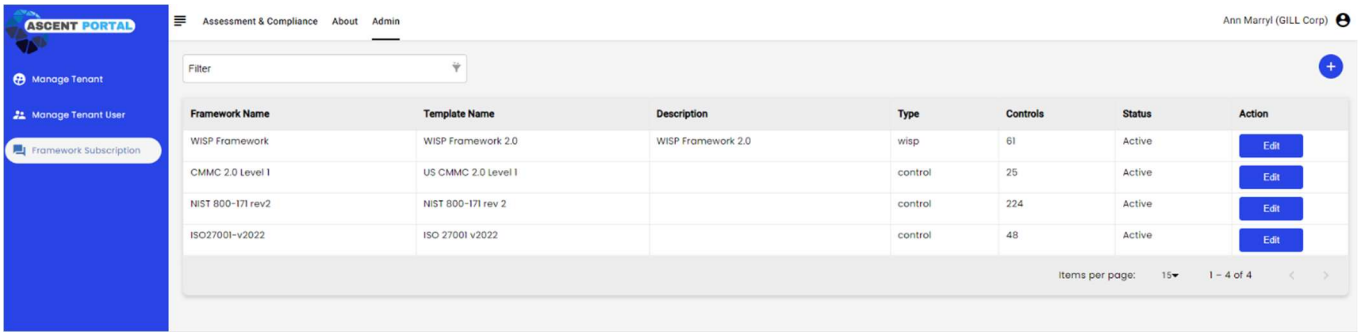
1. The user will receive a welcome email from the ASCENT Portal.
2. Open the welcome email and click the password reset link within.
3. Follow the instructions on the password-setting page to create a new password for the user account.

How to assign frameworks to a tenant

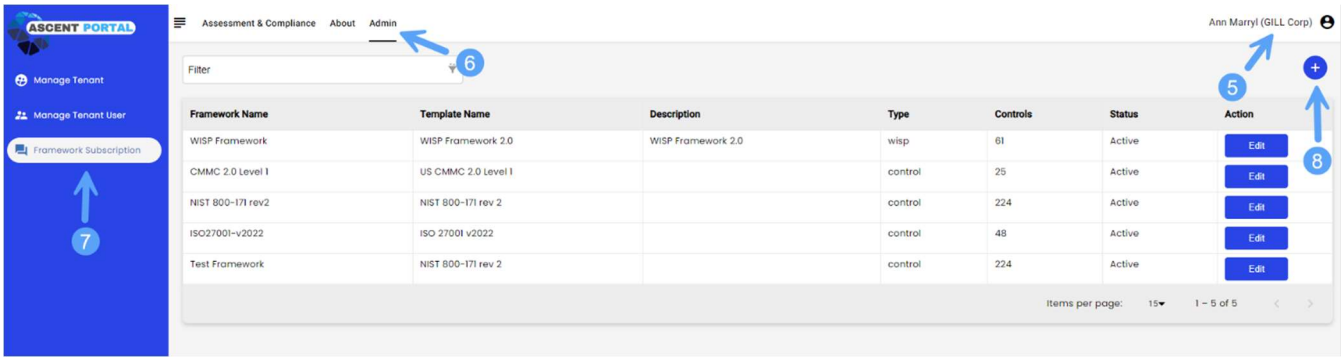
1. Log in to the Portal, which will log you in as the admin for your MSP organization (confirmed by the top right corner, which will state which organization you are logged in as) (1).
2. Click **Admin** (2).
3. Click **Manage Tenant** (3).
4. Click **Switch,** corresponding to the tenant you need to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



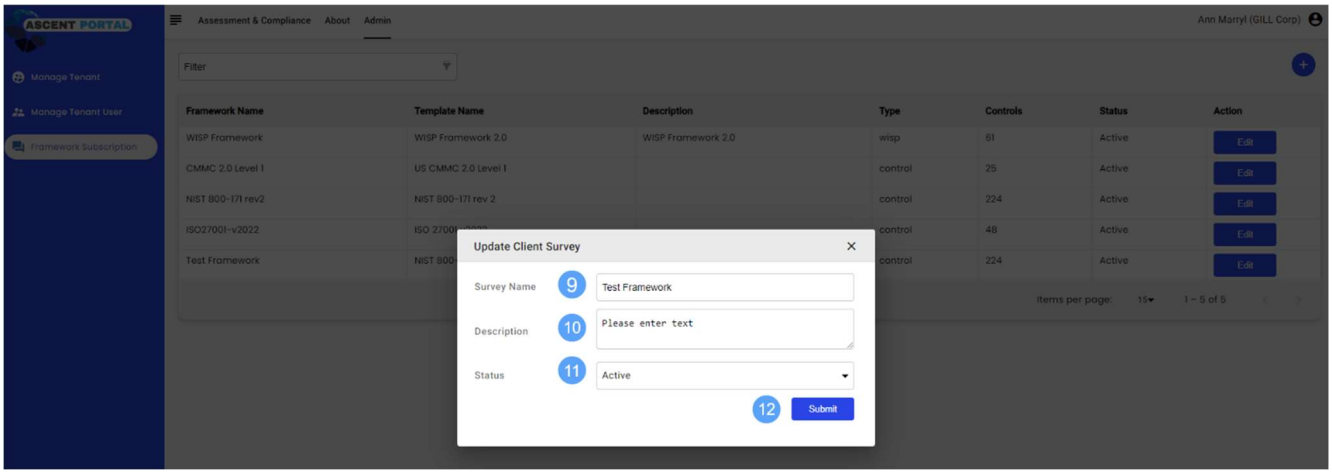
5. Now that you are in the tenant's Portal (confirmed in the top right corner by stating the company's name) (5), click **Admin** (6).
6. Click **Framework Subscription** (7).
    a. Here you will see the current frameworks assigned to this Portal and details for each framework.



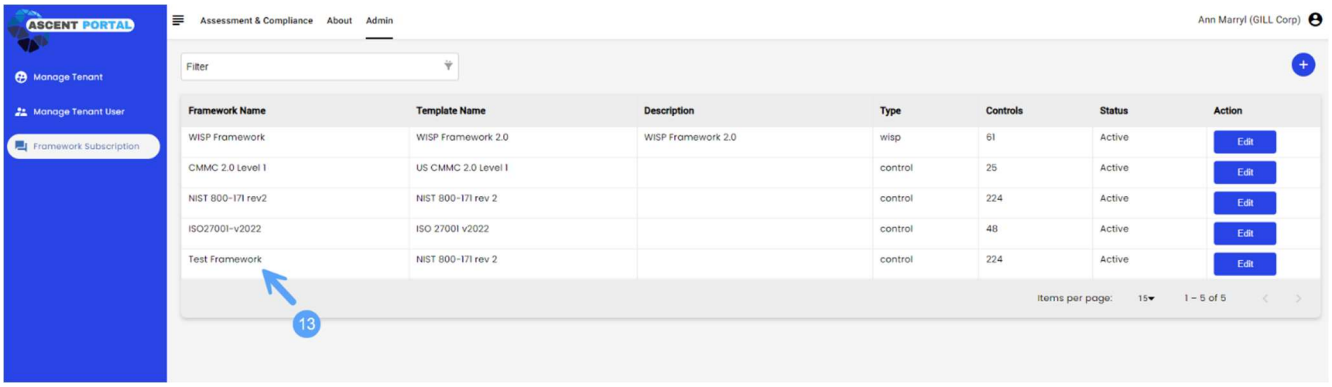
7. Click the **plus sign** (8).



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).

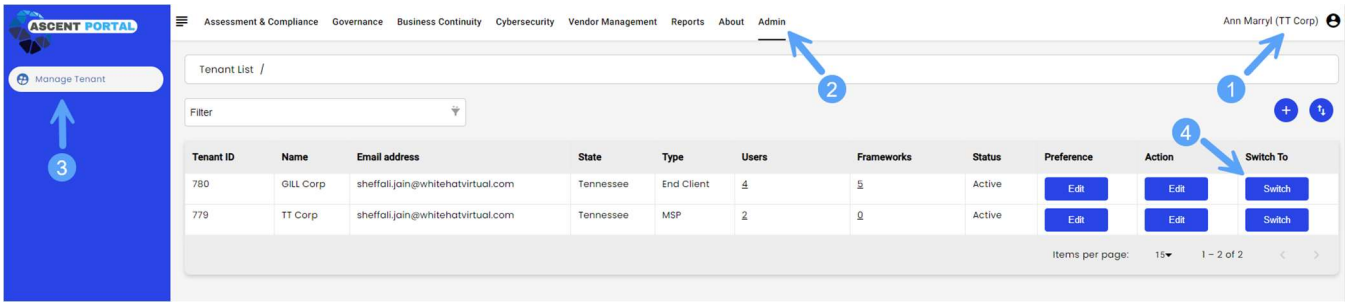


You'll see the newly assigned framework now in the list (13).

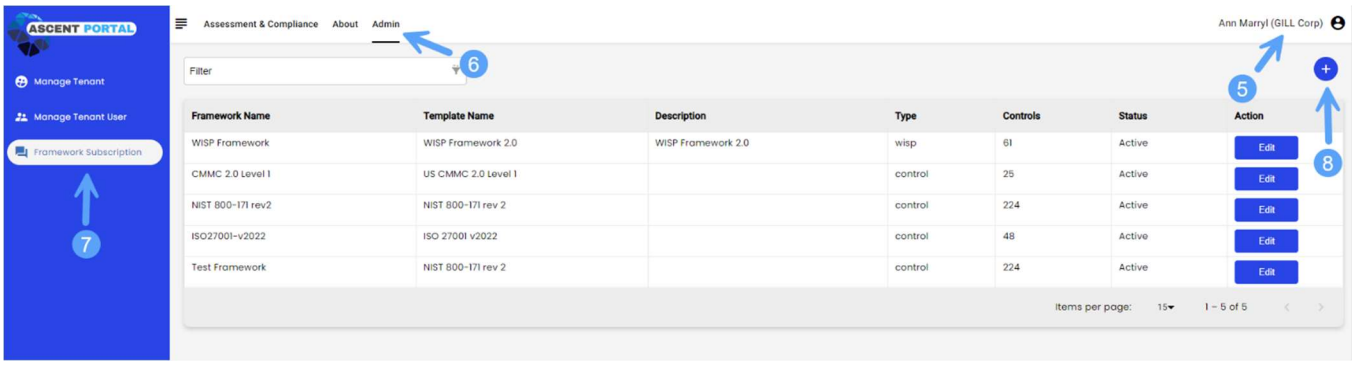


How to deactivate a framework for a tenant

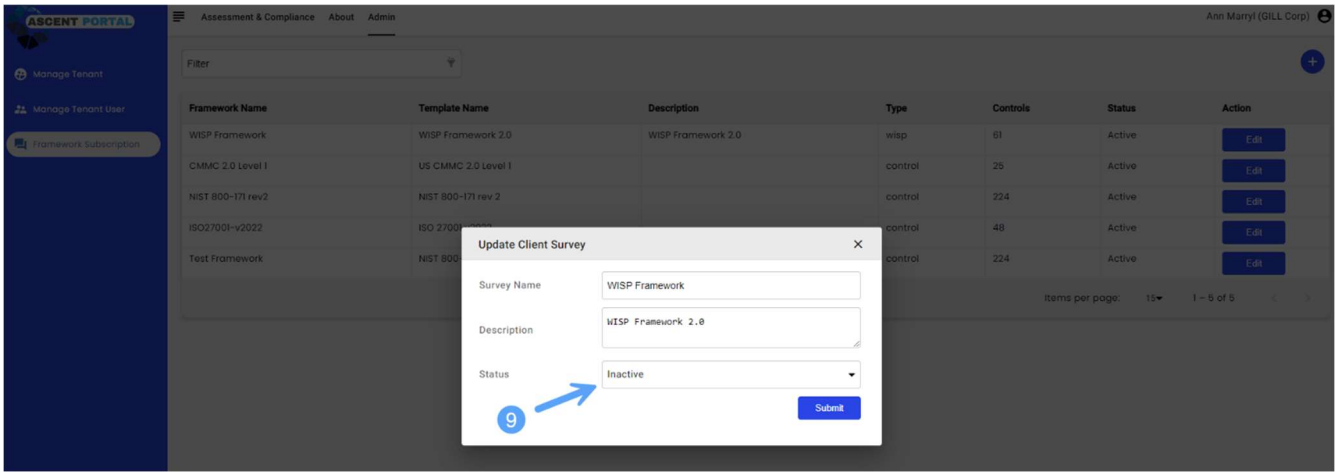
1. Log in to the Portal, which will log you in as the admin for your MSP organization (confirmed by the top right corner, which will state which organization you are logged in to) (1).
2. Click **Admin** (2).
3. Click **Manage Tenant** (3).
4. Click **Switch,** corresponding to the tenant you need to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



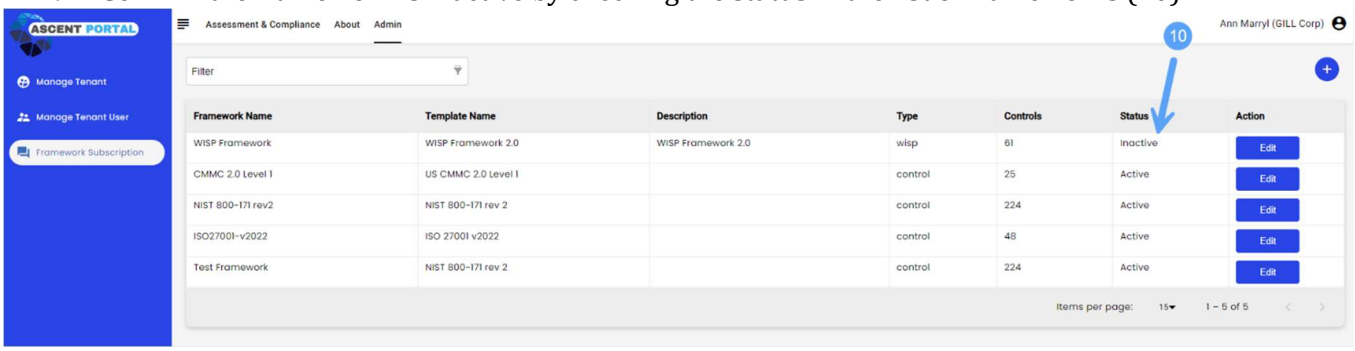
5. Now that you are in the tenant's Portal (confirmed in the top right corner by stating the company's name (5), click **Admin** (6).
6. Click **Framework Subscription** (7).
    a. Here you will see the current frameworks assigned to this Portal, and details for each framework.
7. Click **Edit** next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



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

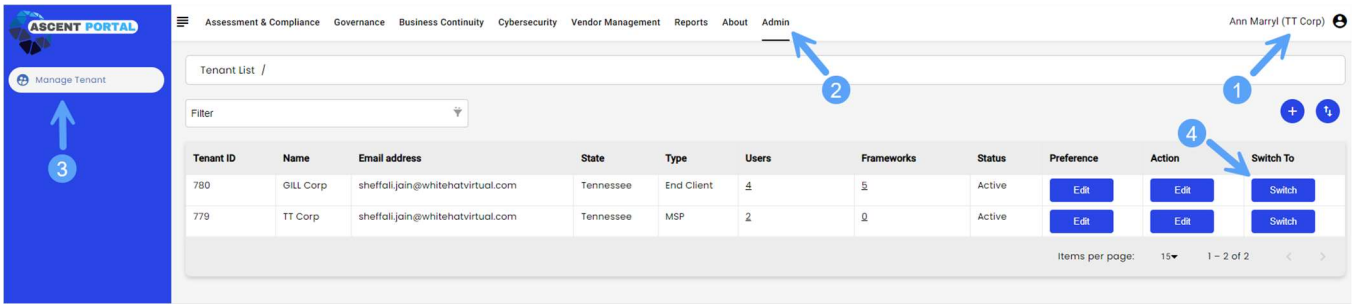


9. Confirm the framework is inactive by checking the status in the list of frameworks (10).

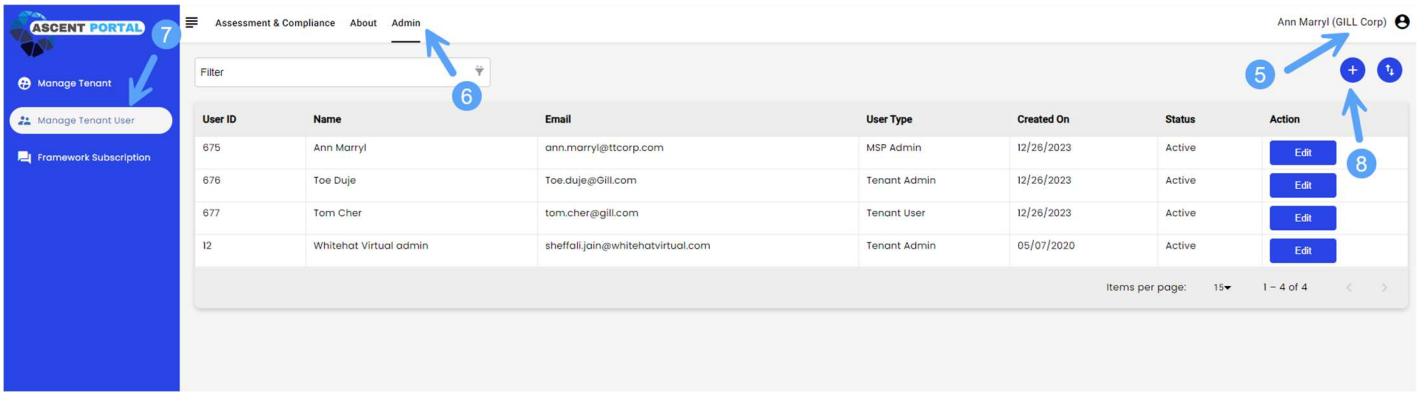


How to set access types for a new user within a tenant

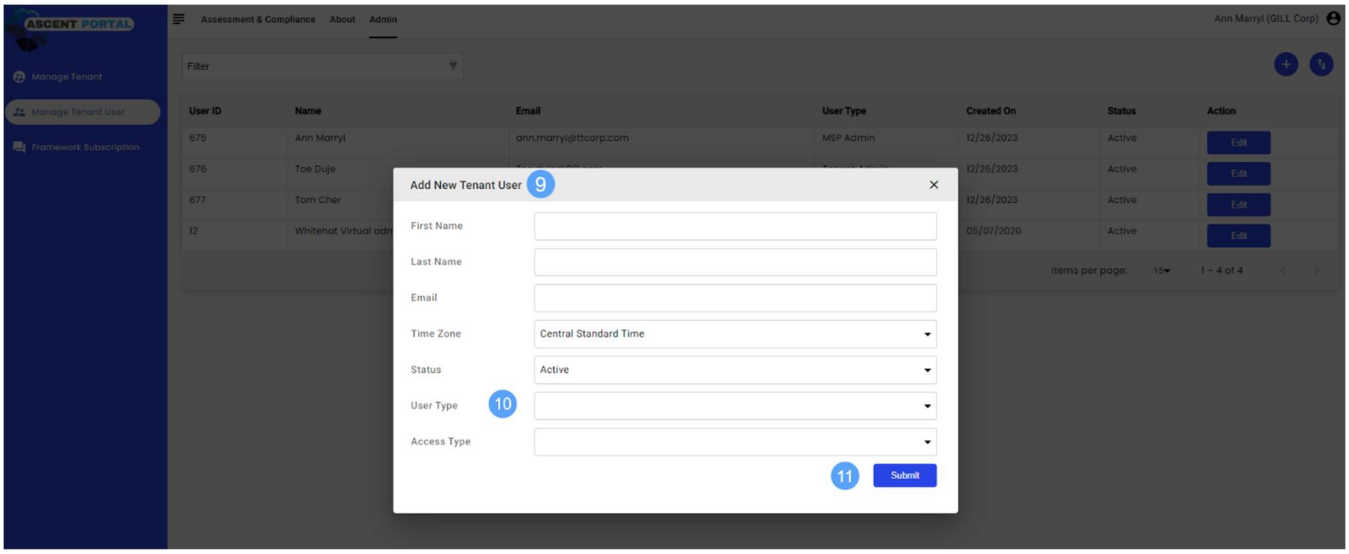
1. Log in to the Portal, which will log you in as the admin for your MSP organization (confirmed by the top right corner, which will state which organization you are logged in to) (1).
2. Click **Admin** (2).
3. Click **Manage Tenant** (3).
4. Click **Switch,** corresponding to the tenant you need to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



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).



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).

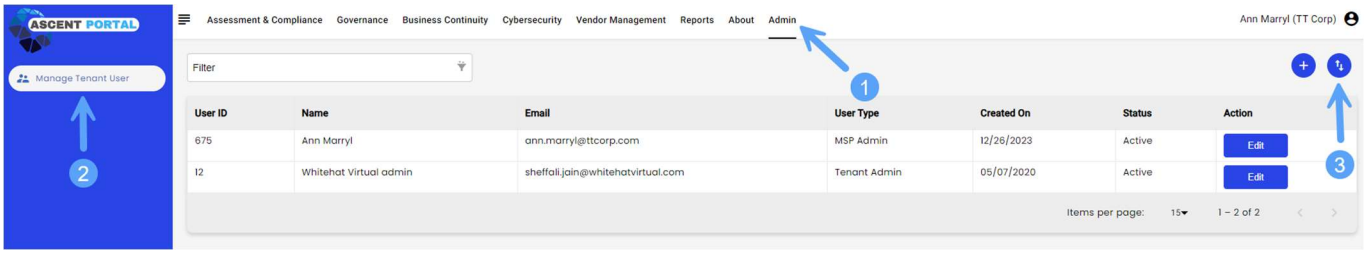


11. A new user email will be sent to the new user from the Portal.

How to export Tenant details in excel format

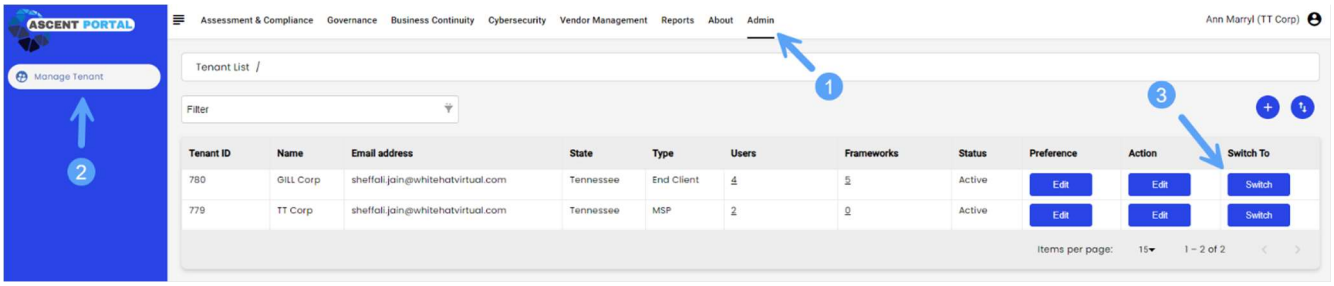
To pull an excel report of the tenants and users within the tenants, follow these steps:

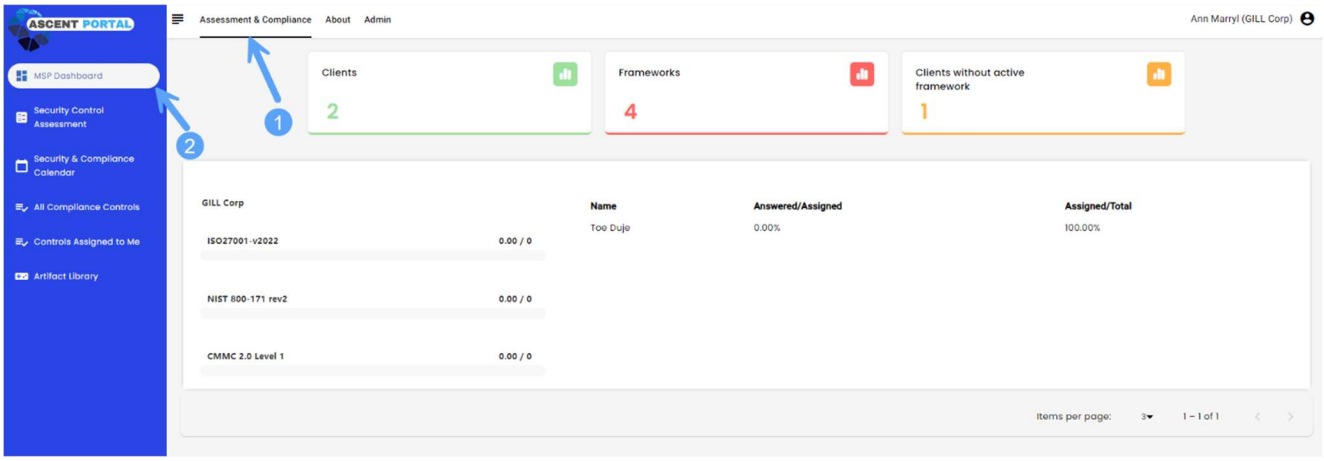
1. Click **Admin** (1).
2. Click **Manage Tenant User** (2).
3. Click the **export icon** (3).
4. An excel file will download to your downloads folder.



How to view a compliance score of a tenant

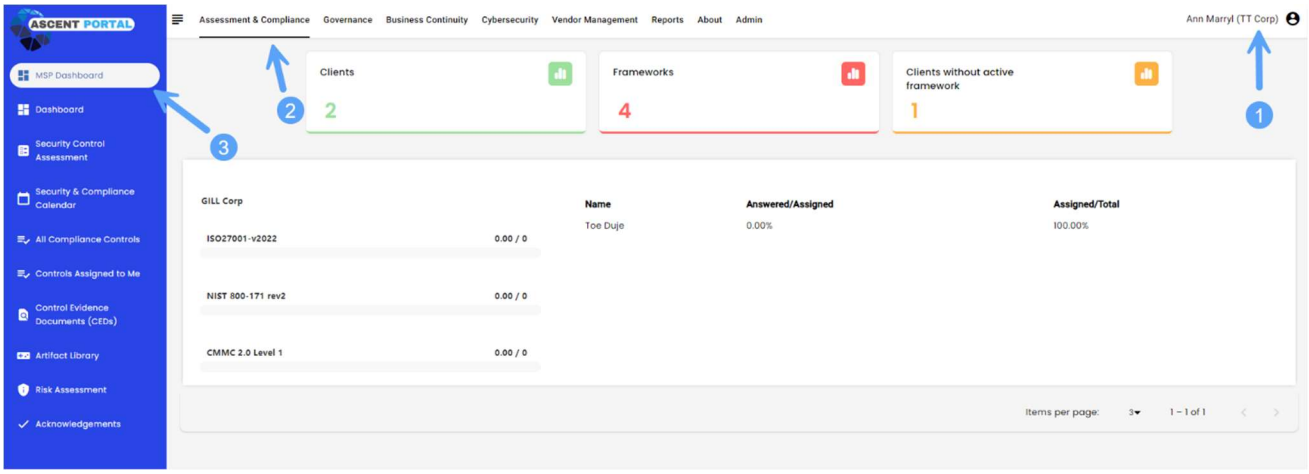
1. Click **Admin** (1)
2. Click **Manage Tenant** (2)
3. Click **Switch** (3) associated with the tenant you would like to review.
4. Click **Assessment & Compliance** (4)
5. Click **MSP Dashboard** (5)
6. You also can now view the score from this MSP Dashboard.





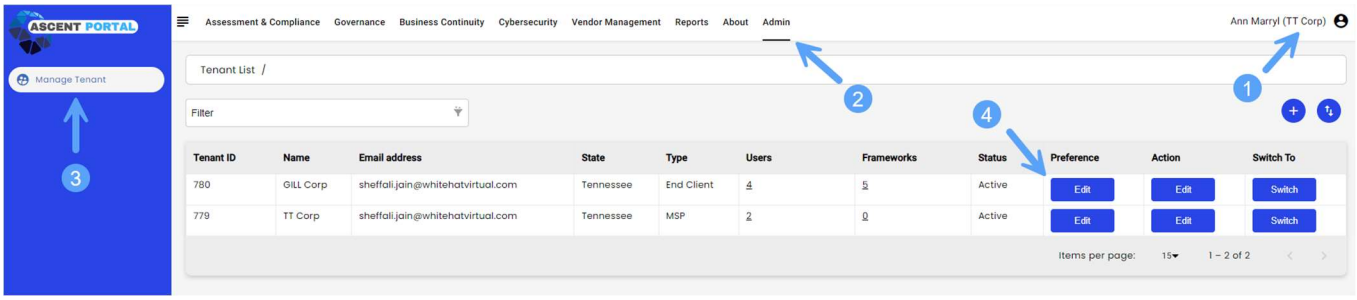
How to create a summary of compliance scores for all tenants

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.

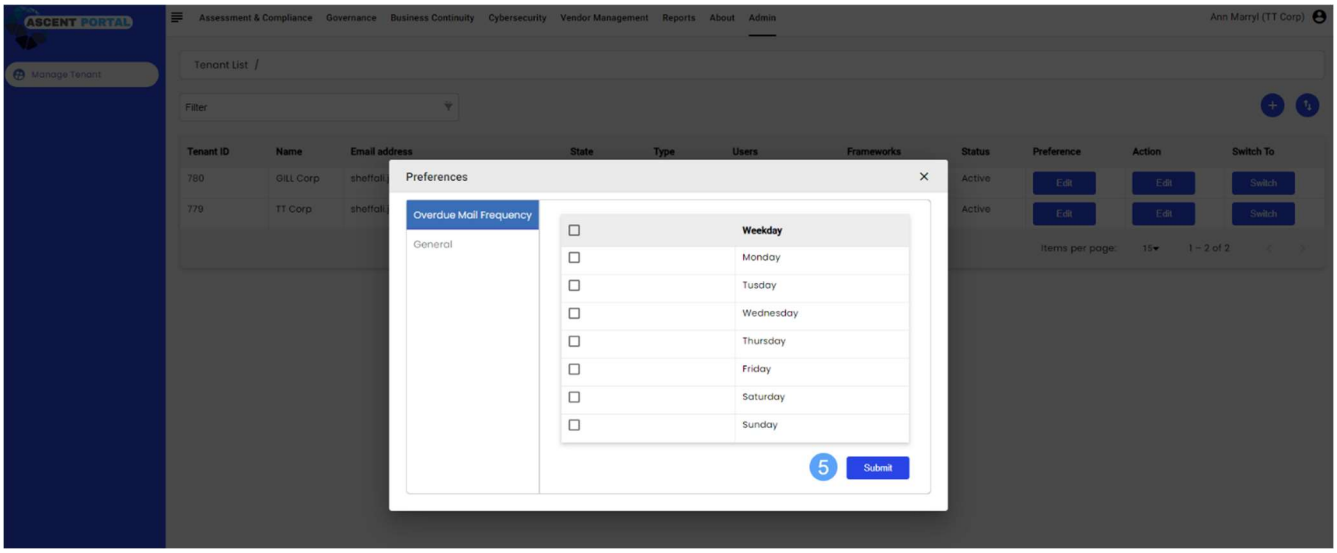


How to set overdue control automatic email frequency for a tenant

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).

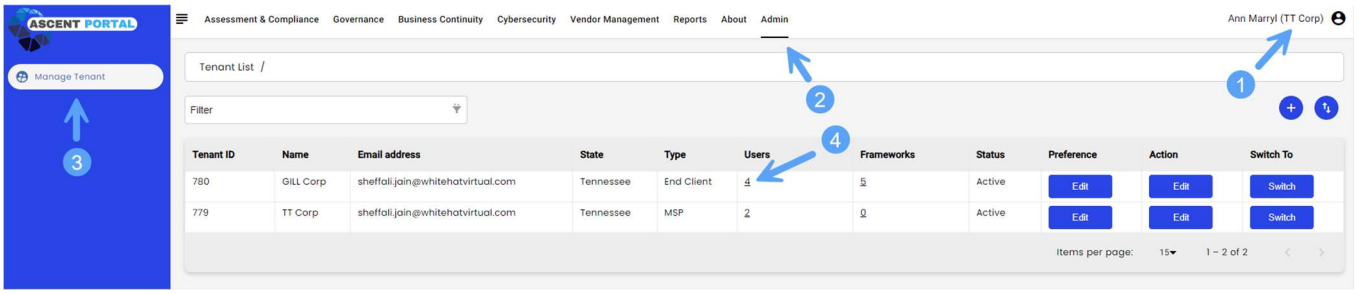


5. In the pop-up, choose which day(s) the Portal will be allowed to email overdue control alerts to users, and click **Submit** (5).

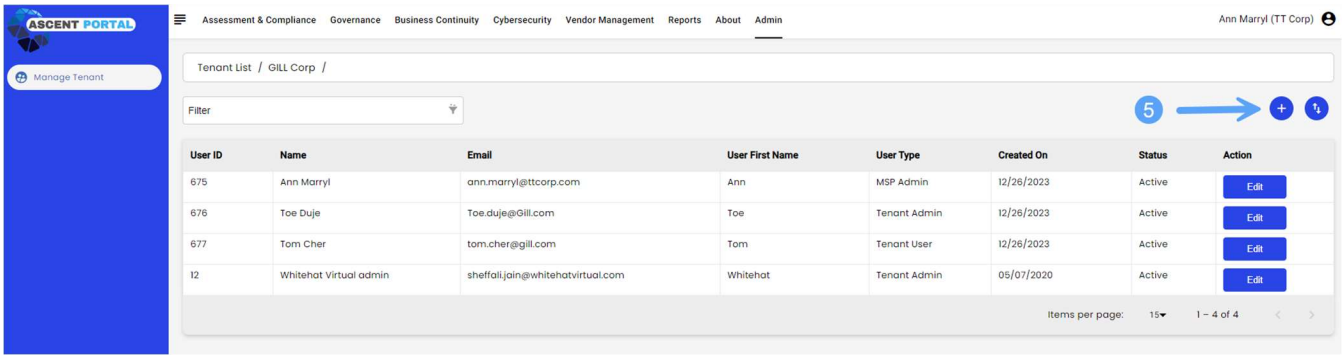


How to add an Internal/External Auditor to the Portal

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).



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



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