

# GRC Platform with AI

Simplify Cybersecurity

Compliance Management



Compliance



Multi-Tenant



Attack Surface



Vendor Management



Generative AI



Dashboards



Ticket Management



Data Protection





# Risk Cognizance

Your Comprehensive Governance Risk and Compliance (GRC), Attack Surface, and Ticket Management System

Why Risk Cognizance Is Important For Your Business's Cybersecurity

- **Comprehensive Platform:** Risk Cognizance is a powerful GRC platform that enhances your cybersecurity and compliance posture.
- **Versatile Capabilities:** Offers robust features for governance, risk management, compliance, attack surface analysis, and ticket management.
- **Smart Investment:** Essential for businesses serious about cybersecurity and compliance.
- **Scalable Solution:** Suitable for businesses of all sizes, ensuring your organization remains secure and compliant.





# What is a GRC Platform?

GRC (Governance, Risk, and Compliance) Platform: An integrated suite of tools designed to streamline and manage governance, risk management, and compliance processes within an organization.



## Key Components:

- **Governance:**
  - Policy Management
  - Audit Management
  - Performance Management
- **Risk Management:**
  - Risk Identification
  - Risk Assessment
  - Risk Mitigation
  - Risk Monitoring
  - Vulnerability Monitoring
  - Vendor Risk Management
- **Compliance:**
  - Regulatory Compliance
  - Internal Controls
  - Incident Management
  - Reporting



# Why Risk Cognizance GRC Platform?.

Cost effective 5 solutions in one system

Interconnected Process management

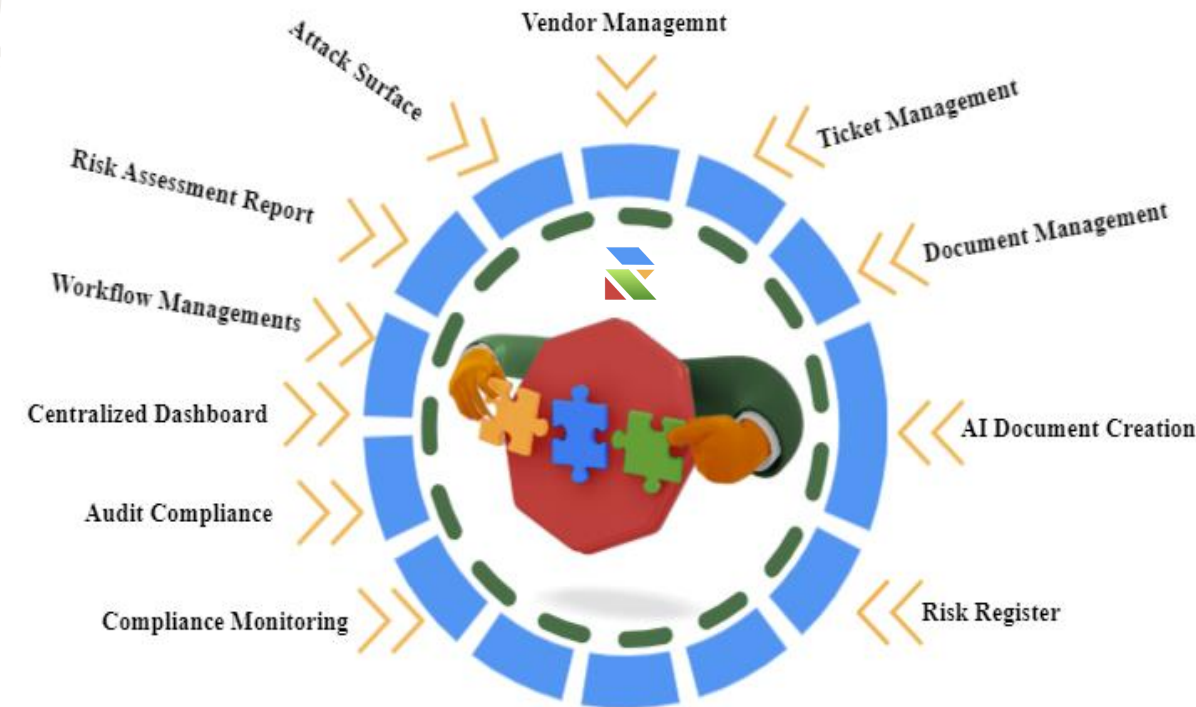
Data and Reporting Automation

Save Time, Money & Resources



# Key Features of Risk Cognizance

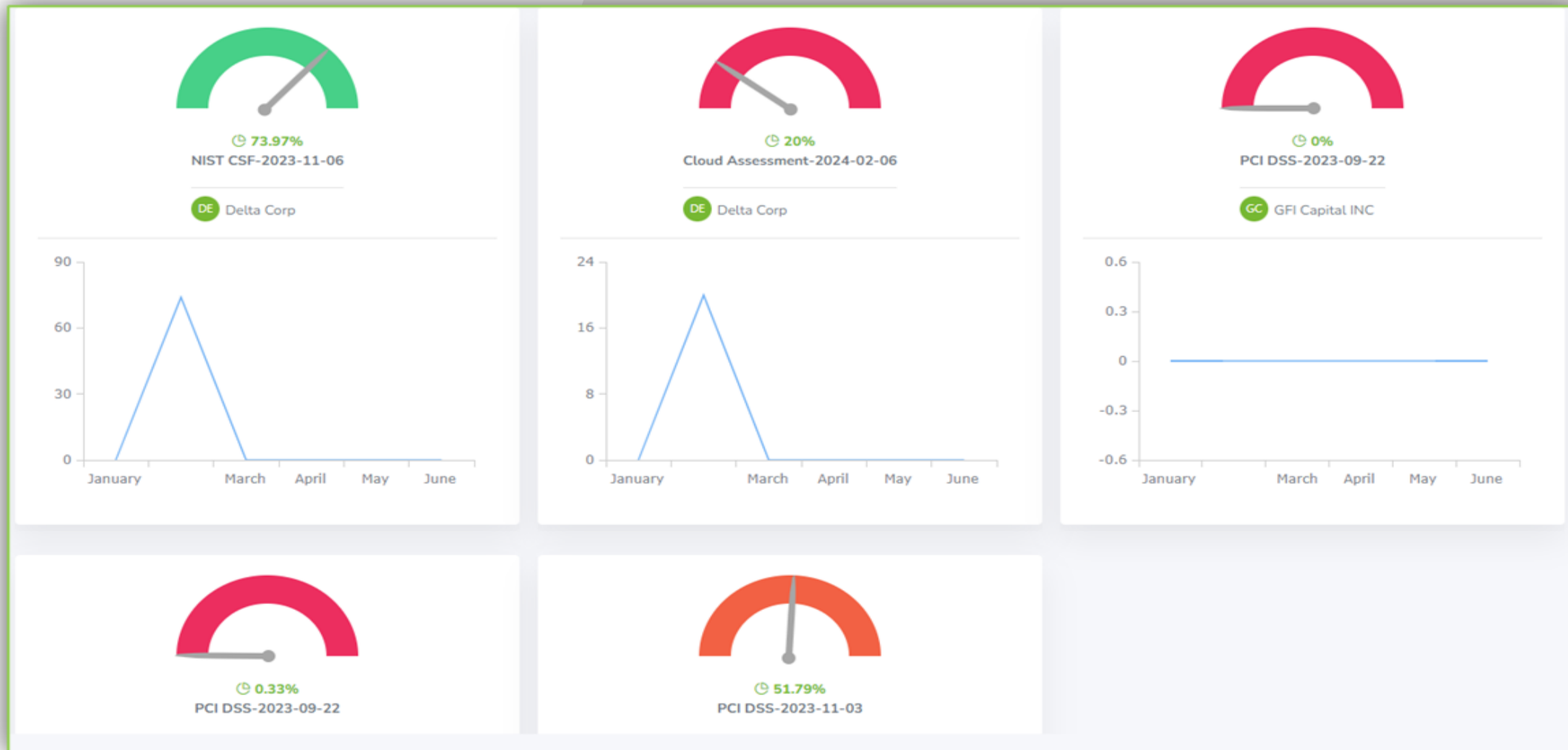
- **Integrated Dashboards and Workflow Automation:** Comprehensive views and streamlined processes to reduce manual effort.
- **Document Management:** Secure organization, storage, and retrieval of essential documents.
- **Risk Scoring and Compliance Tracking:** Evaluating and prioritizing risks and monitoring adherence to various regulations.
- **Audit Trails and Incident Reporting:** Detailed logs for transparency and efficient management of compliance incidents.
- **Multi-Tenant and Multiple Framework Support:** Manage multiple clients or divisions and support various compliance frameworks.
- **Vendor and Access Management:** Efficient third-party risk management and detailed access tracking.
- **Attack Surface and Ticket Management:** Identify potential vulnerabilities and streamline issue tracking and resolution.





# Manage Multiple Framework

Risk Cognizance is a multi-tenant and multi-framework platform that provides scalable solutions for governance, risk, and compliance.





# Supporting Frameworks and Regulatory Requirements

**Risk Cognizance is committed to adhering to robust frameworks and regulatory standards to ensure comprehensive risk management and compliance.**

- Cloud Assessment Frameworks
- NIST CSF
- SOC 2
- GBLA
- CIS V8
- SOC 1
- HIPAA
- ISO 27001
- NIST 800-53
- FedRamp
- CMMC
- PCI DSS
- GDPR
- Additional Frameworks

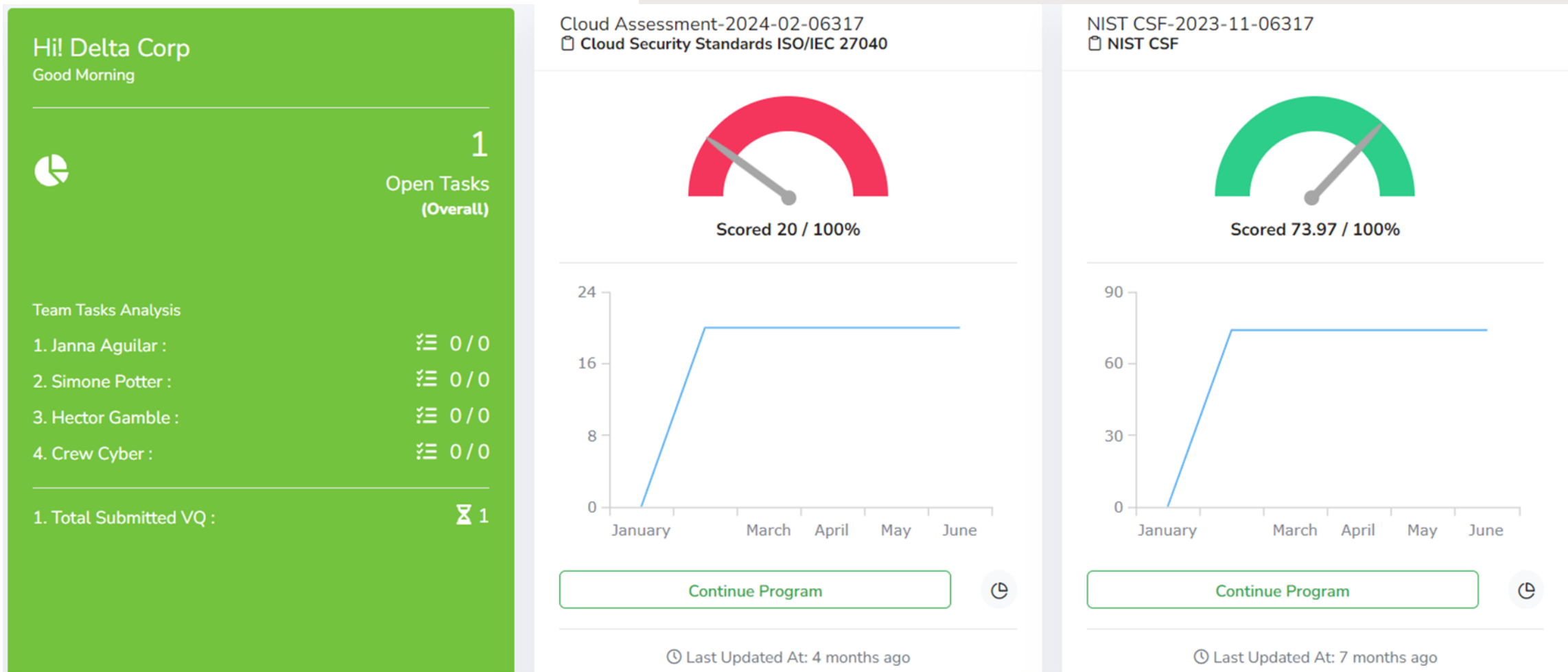






# Client Compliance Dashboard

Get insight into the overall compliance program dashboard.

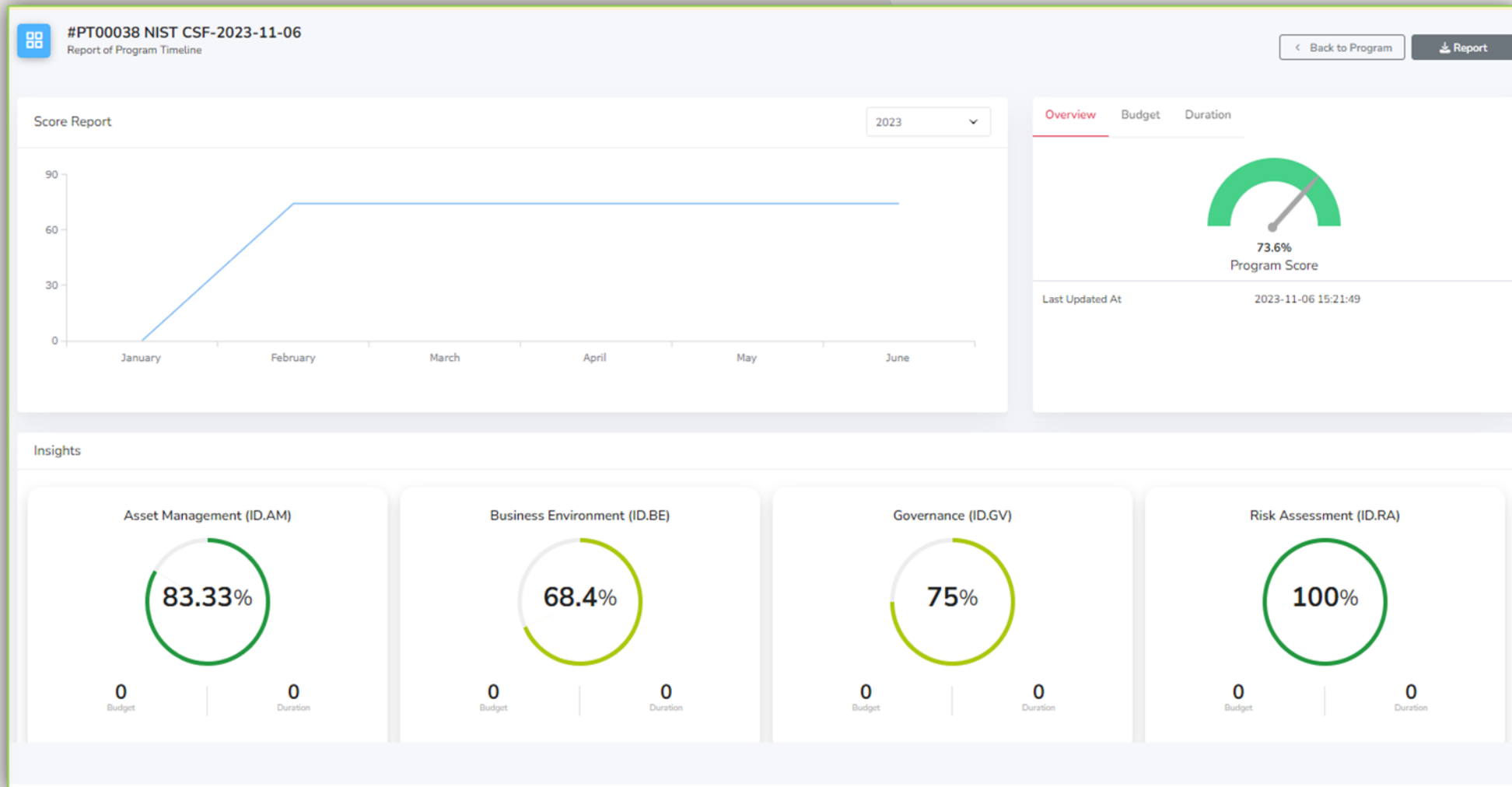






# Compliance Reporting

Get insight into the overall compliance program reporting.





# Vendor Questionnaire

Streamline vendor and supplies assessment to ensure trust and integrity



Vendor Management

NIST CSF-2024-02-21

5.09% Score  
Progress: 8.33%

Access has been granted to IBM on behalf of Delta Corp to submit the vendor questionnaire for Receptionist NIST CSF-2024-02-21.

**Accepted**  
The NIST Cybersecurity Framework (CSF) Assessment is a tool used to evaluate an organization's cybersecurity...

I hereby confirm that all information provided in the questionnaire has been accurately and validly completed.

**Submit Questionnaire**

Thank you IBM for taking participation in our vendor questionnaire program.

**Asset Management (ID.AM)** (4 of 6) ▼  
Last Modified 27-06-2024

Do you inventory physical devices and systems within our organization?  
Subcontrol : Device and System Management (ID.AM-1) ⓘ

Options \* ⓘ  
 Yes  
 No  
 Partially  
 Not Applicable  
 I Don't Know

Note ⓘ  
Enter Notes

Recommendation ⓘ

Files  
Attach Documents (0)

Do you inventory software platforms and applications within the organization?  
Subcontrol : Software and Applications Management (ID.AM-2) ⓘ

Options \* ⓘ  
 Yes  
 No  
 Partially  
 Not Applicable  
 I Don't Know

Note ⓘ  
Enter Notes

Recommendation ⓘ



# Risk Register Reporting

Get insight into the overall compliance program reporting



Risk Profiling

**Risk Register Report (R3)**  
 | NIST CSF-2023-11-06 (NIST CSF)  
 Started on: 2023-11-06 14:29:50 | Last Updated on: 2023-11-06 15:21:43

Client Name  
Delta Corp

**Insights**

Area	1 - NEGLIGIBLE/MINIMAL	2 - LOW/MINOR	3 - MODERATE	4 - HIGH/MAJOR	5 - EXCESSIVE/CATASTROPHIC
Inherent Impact	1	0	0	0	0
Residual Impact	1	0	0	0	0
Inherent Likelihood	1	0	0	0	0
Residual Likelihood	1	0	0	0	0

Status	Count
Identified	1
Analysis Complete	0
Planning	0
Planning Complete	0



# Teams Calendar and Task List

Timely workflow process with task and calendar



## Task Management

ID	Task Priority	Status	Member	Date	Assign By
#T00055	Audit User Access High	For Review	Hector Gamble	01-11-2025	Delta Corp 02-07-2024
#T00055	Audit User Access High	For Review	Hector Gamble	01-09-2026	Delta Corp 02-07-2024
#T00055	Audit User Access High	For Review	Hector Gamble	01-07-2027	Delta Corp 02-07-2024
#T00055	Audit User Access High	For Review	Hector Gamble	01-05-2028	Delta Corp 02-07-2024
#T00055	Audit User Access High				
#T00055	Audit User Access High				
#T00054	Access Policy Audit Medium				
#T00054	Access Policy Audit Medium				
#T00054	Access Policy Audit Medium				
#T00054	Access Policy Audit Medium				

Teams Calendar							All Members	▼	☰
All Members tasks									
June 2024							Month	Week	Day
Sun	Mon	Tue	Wed	Thu	Fri	Sat			
26	27	28	29	30	31	1			
2	3	4	5	6	7	8			
9	10	11	12	13	14	15			
					Audit Firewall @Crew Cyber				



# Prebuilt Policy Templates

Pre-built cybersecurity policies that you can use to quickly establish robust security frameworks, ensuring compliance and reducing the risk of cyber threats.



## Prebuild Policies

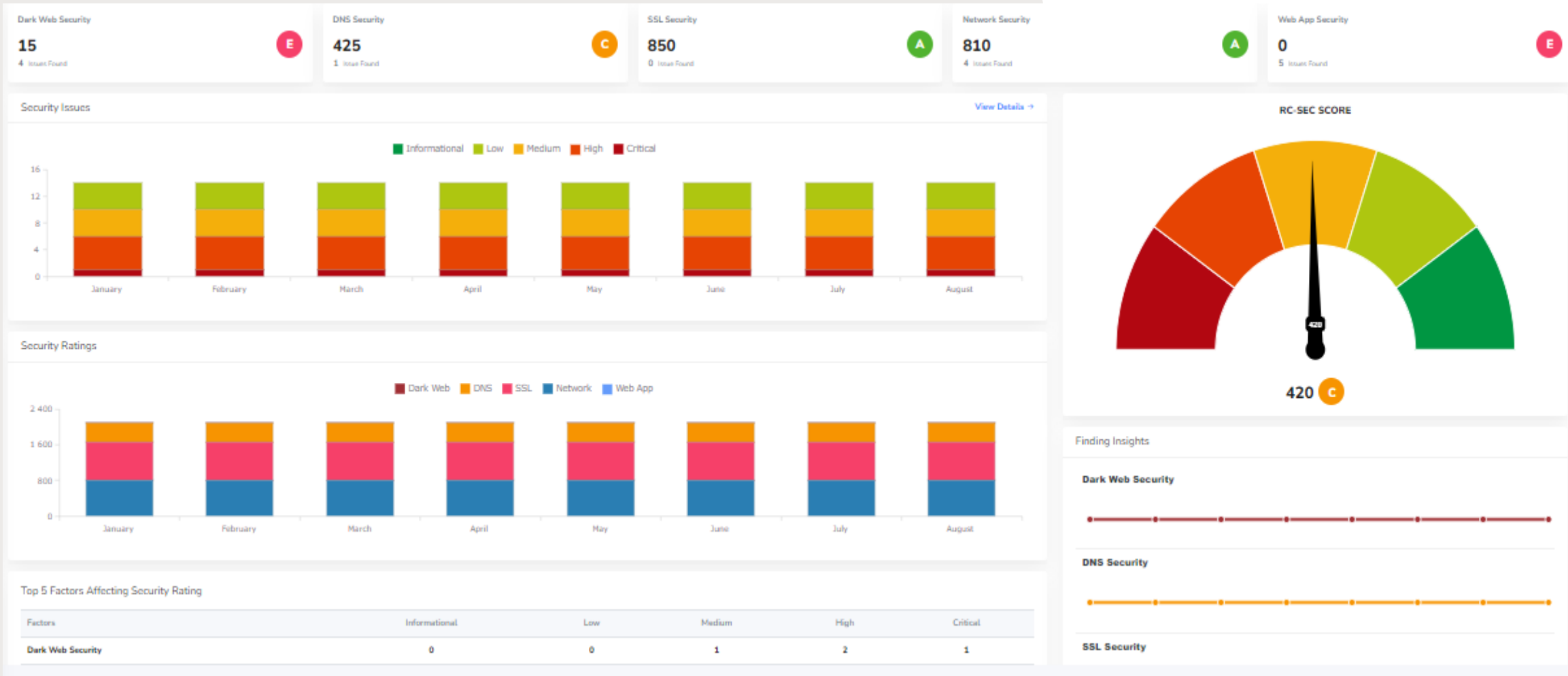
Policy Template

Show  entries

<input type="checkbox"/> Actions	#	Title	Status
<input type="checkbox"/> ⋮	<a href="#">#RA00893</a>	Data Breach Response Policy	<a href="#">Publish</a>
<input type="checkbox"/> ⋮	<a href="#">#RA00892</a>	Wireless Communication Policy	<a href="#">Publish</a>
<input type="checkbox"/> ⋮	<a href="#">#RA00891</a>	Bluetooth Baseline Requirements Policy	<a href="#">Publish</a>
<input type="checkbox"/> ⋮	<a href="#">#RA00890</a>	Disaster Recovery Plan Policy	<a href="#">Publish</a>
<input type="checkbox"/> ⋮	<a href="#">#RA00889</a>	Acquisition Assessment Policy	<a href="#">Publish</a>
<input type="checkbox"/> ⋮	<a href="#">#RA00888</a>	Artificial Intelligence Policy	<a href="#">Publish</a>

# Attack Surface Management (ASM)

We mitigate ongoing risks with our comprehensive attack surface management solutions.



# Dark Web Monitor

Dark web monitoring is a proactive cybersecurity security tool searching and monitoring information on the dark web that can potentially be used to breach your organization.



780 **A**

Latest Scan: 09 Aug, 2024

## Dark Web Monitor Report

Last Scanned: 8/22/2024



### 3 Unique Findings



### Findings Summary

Severity	Findings	Factor	Score Impacted	Occurrence
Critical	Sensitive Email & Password Breach Detected	Dark Web Security	-60 PTS	3
High	Contact Information Disclosed	Dark Web Security	-10 PTS	1

- Identify exposed credentials and sensitive data early.
- Prevent cyberattacks by detecting dark web threats.
- Protect your organization's reputation by stopping breaches.
- Stay ahead of cybercriminals trading stolen information.
- Strengthen cybersecurity by quickly addressing vulnerabilities.





# Document Management with AI

Streamlines document creation by automating policy drafting, ensuring compliance, and enhancing procedural accuracy



GENERATIVE AI

### Add Ai Resource Article

Add a new record for Ai Resource Article

Home / Ai Resource Article

#### Add Ai Resource Article

Step 1. Choose Format

Composer Manually  Use Ai Builder

Description \*

I am here to help you create document and policies

Submit

### Information Security Policies

- Remote Policy
- Security Policy

## Q. Security Policy

Document Name: Security Policy

Type: Group to Whom It Applies: Staff within the Trust Scope: Whole of the Trust Access: Date: 2013 Review: 2015 Reviewed By: Management Team, Manager – IM&T Infrastructure Leads: Director of Finance/Deputy Chief Executive For Advice: Manager, Performance & Information Department

### NETWORK SECURITY POLICY

#### 1. Introduction

1.1 This document defines the Network Security Policy for South West Yorkshire Partnership NHS Foundation Trust (referred to hereafter as the Trust). The Network Security Policy applies to all business functions and information contained on the network, the physical environment, and relevant people who support and are Users of the network.

1.2 This document: a. Sets out the Trust's policy for the protection of the confidentiality, integrity, and availability of the network; b. Establishes the security responsibilities for network security; c. Provides reference to documentation relevant to this policy.

1.3 The network is a collection of communication equipment such as servers, computers, printers, and modems, which has been connected together by cables or wireless devices. The network is created to share data, software, and peripherals such as printers, modems, fax machines, Internet connections, CD-ROM and tape drives, hard disks, and other data storage equipment.

#### 2. Purpose/Scope of this Policy

2.1 The purpose of this policy is to ensure the security of The Trust's network. To do this, the Trust will: a. Ensure Availability Ensure that



# Document Management with Drag and Drop

Streamline document management to ensure trust and integrity



Document Management

The screenshot displays a web interface for 'My Library'. The header includes the title 'My Library' and a subtitle 'List of My Library'. On the right side of the header, there is a search bar labeled 'Search By Name...' and a green button labeled 'Upload New Document'. The main content area is a grid of document thumbnails. Each thumbnail shows a file icon (e.g., PDF, DOCX, XLS, TXT, image), a filename, and a small red square icon in the top right corner. The files listed include: 'J and J Trucking and Haul...', 'upmychain-img-01', 'file-sample\_100kB-(2)', 'SampleCSVFile\_2kb', 'file\_example\_XLSX\_10 (1)', 'Leaves', 'hello', 'apaluxurycarrental.com\_li...', 'DWSample1-TXT', 'New Microsoft Word Docume...', 'hall of fame (1)', 'New Microsoft Word Docume...', and 'New Microsoft Excel Works...'.



# Ticket Management

Ensure integration of support and task manage with tickets and task



Support Ticket Management

Support Tickets

From mm/dd/yyyy To mm/dd/yyyy Select Status

Show 10 entries Search

Actions	#	Subject	Status	Created At
<input type="checkbox"/> ⋮	#ST00053	Facing problems using their system	Close	4th Nov, 2023 11:24 AM
<input type="checkbox"/> ⋮	#ST00033	General Support	Close	29th Oct, 2023 15:42 PM
<input type="checkbox"/> ⋮	#ST00023	General Support	Awaiting Reply	26th Sep, 2023 12:13 PM
<input type="checkbox"/> ⋮	#ST00021	General Support	Awaiting Reply	26th Sep, 2023 11:55 AM
<input type="checkbox"/> ⋮	#ST00019	Facing problems using their system	Awaiting Reply	26th Sep, 2023 11:54 AM
<input type="checkbox"/> ⋮	#ST00018	Facing problems using their system	Awaiting Reply	26th Sep, 2023 11:53 AM
<input type="checkbox"/> ⋮	#ST00012	General Support	Close	23rd Sep, 2023 02:45 AM



# License Management

## Risk and Provider Control (RPC)

This framework allows Managed Security Service Providers (MSSPs) to control licenses for their clients and track assets for attack surface, and vendor management. RPC integrates with existing systems and tools to provide a seamless experience for license and asset management.

## Key Advantages:

- **License Management:** Allows MSSPs to manage and control licenses for their clients, ensuring compliance and optimal use of licensed resources.
- **Asset Tracking:** Enables the tracking of client asset licenses provided by the MSSP, offering visibility for billing and approval of additional licenses.
- **Vendor Oversight:** This feature facilitates the tracking of vendor management licenses provided to clients by the MSSP. It provides visibility for billing and supports the approval process for acquiring additional licenses.

The screenshot displays the RPC interface. The top left panel shows a shield icon, a '1850 RCP' balance, a 'Request RCP' button, and 'Plan Validity Till : 8th Jan, 2026'. The top right panel is a 'RCP Transaction' form with a close button, a text input for 'How much RCP you want to add?', a 'Request' button, and 'Your current wallet amount : RCP 1850'. Below these is a table with columns: '#', 'Amount', 'Remark', 'Created At', and 'Status'. The table contains 7 rows of transaction data.

#	Amount	Remark	Created At	Status
1	-RCP1.00	For Assigning Aug test questionnaire (#36) to Delta Corp (#317)	2024-08-02 06:21:12	Accepted
2	+RCP1.00	All Covered Inc have request for amount RCP1.00	2024-08-01 04:31:01	Declined
3	+RCP1.00	Your request for RCP's has been accepted by the system with an amount of RCP1.00.	2024-08-01 04:30:19	Accepted
4	+RCP500,022.00	All Covered Inc have request for amount RCP500,022.00	2024-08-01 04:28:09	Declined
5	+RCP50,000.00	All Covered Inc have request for amount RCP50,000.00	2024-08-01 04:26:37	Declined
6	-RCP1.00	For Assigning SIG Lite_VQ (#23) to James Villarreal (#594)	2024-07-31 04:07:19	Accepted
7	-RCP1.00	For Assigning CCPA_VQ (#20) to Pratyush DZE (#586)	2024-07-30 08:00:31	Accepted



# Battle Card

In today's complex risk landscape, organizations need a robust solution to manage their enterprise risks effectively. Risk Cognizance is designed to provide a comprehensive approach that enhances risk management processes and strengthens organizational resilience. As demonstrated in the Battle Card on the right, we outperform our competitors, offering a more comprehensive range of solutions that address the multifaceted nature of risk management more effectively than all other vendors combined.

## Comprehensive Enterprise Risk Management Solution

- Multitenant support
- Vendor management
- Risk register
- Artificial intelligence capabilities
- Attack surface monitoring
- Document management
- Ticket management
- Dark web monitoring
- Calendar and task management

Solutions	Description	Risk Cognizance	Apptega	Audit Board	Risk Profiler	Onetrust
<b>Enterprise Risk Management</b>	Helps large corporations systematically identify, assess, and manage risks at both the operational and strategic levels	●	●	●	○	●
<b>Multitenant</b>	Multi-tenant and multi-framework platform that provides scalable solutions for governance, risk, and compliance	●	●	○	●	○
<b>Compliance</b>	Comprehensive Governance Risk and Compliance (GRC). Supports multiple framework.	●	●	●	●	●
<b>Vendor Management with Attack Surface</b>	Streamline vendor and supplies assessment to ensure trust and integrity.	●	○	●	○	●
<b>Risk Register</b>	Get insight into the overall compliance program reporting with a heat map	●	●	●	○	●
<b>Interactive Artificial Intelligence</b>	Streamline document management to ensure trust and integrity.	●	○	●	○	○
<b>Attack Surface Management</b>	Streamlines document creation by automating policy drafting, ensuring compliance, and enhancing procedural accuracy	●	○	●	●	○
<b>Document Management</b>	Streamline document management to ensure trust and integrity	●	●	●	○	●
<b>Ticket Management</b>	Ensure integration of support and task manage with tickets and task	●	○	○	○	●
<b>Dark Web Monitoring</b>	Dark web monitoring is a proactive cybersecurity tool use for monitoring information on the dark web.	●	○	○	●	●
<b>Pre-build Policies</b>	Pre-built policies that you can use to quickly establish a robust security program.	●	●	●	○	●
<b>Delegation</b>	Revise the delegation code to evaluate a member's access, adding an additional layer of security to the system.	●	○	○	○	○
<b>License Management</b>	Allows MSSPs to manage and control licenses for their clients, ensuring compliance and optimal use of licensed resources.	●	○	○	○	○
<b>Calendar and Task Management</b>	This feature integrates calendar scheduling and task tracking into a single platform	●	○	●	○	●
<b>Self-Management</b>	The solution is flexible, enabling MSSPs to manage frameworks and licenses while clients use an intuitive tool. It also features an integrated ticketing system.	●	○	○	○	○



# The Value of Risk Cognizance

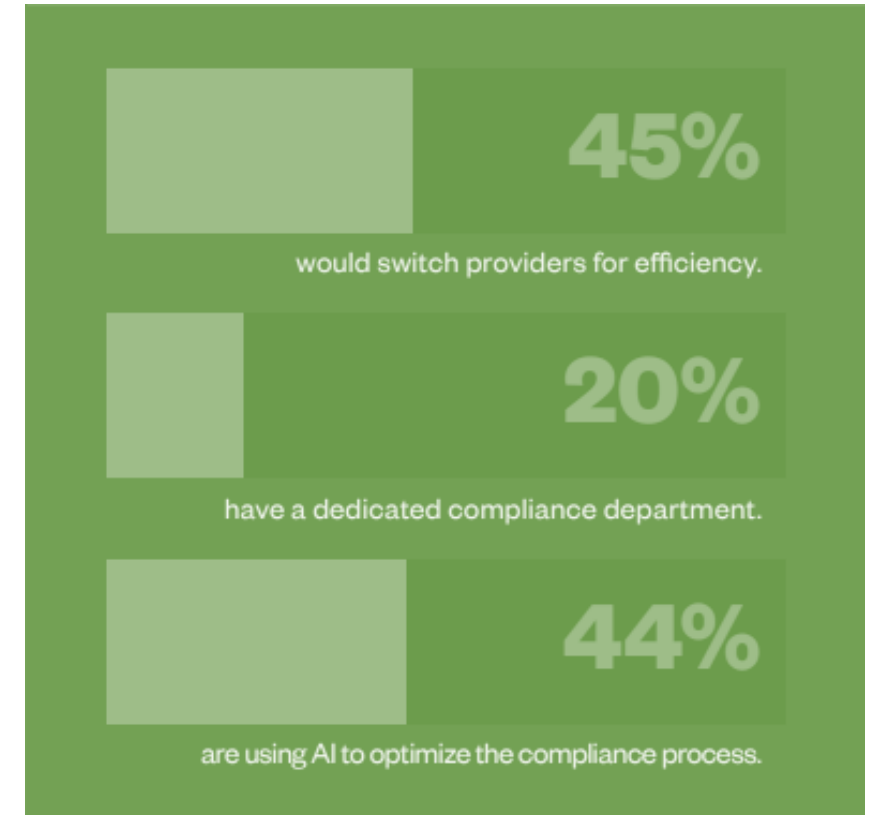
## Transforming Governance, Risk, and Compliance Management

Combining GRC, Attack Surface Management, and Ticket Management into a single tool streamlines automation, ensures compliance, and saves valuable time and resources.

### Key Advantages:

- Unified Platform for GRC, Attack Surface, and Ticket Management
- Real-Time Risk Scoring and Analytics
- Automated Compliance and Workflow Processes
- Proactive Threat Identification and Mitigation
- Resource Optimization and Cost Savings
- Scalability for Growing Businesses
- Enhanced Internal and External Collaboration

## Why others made the switch



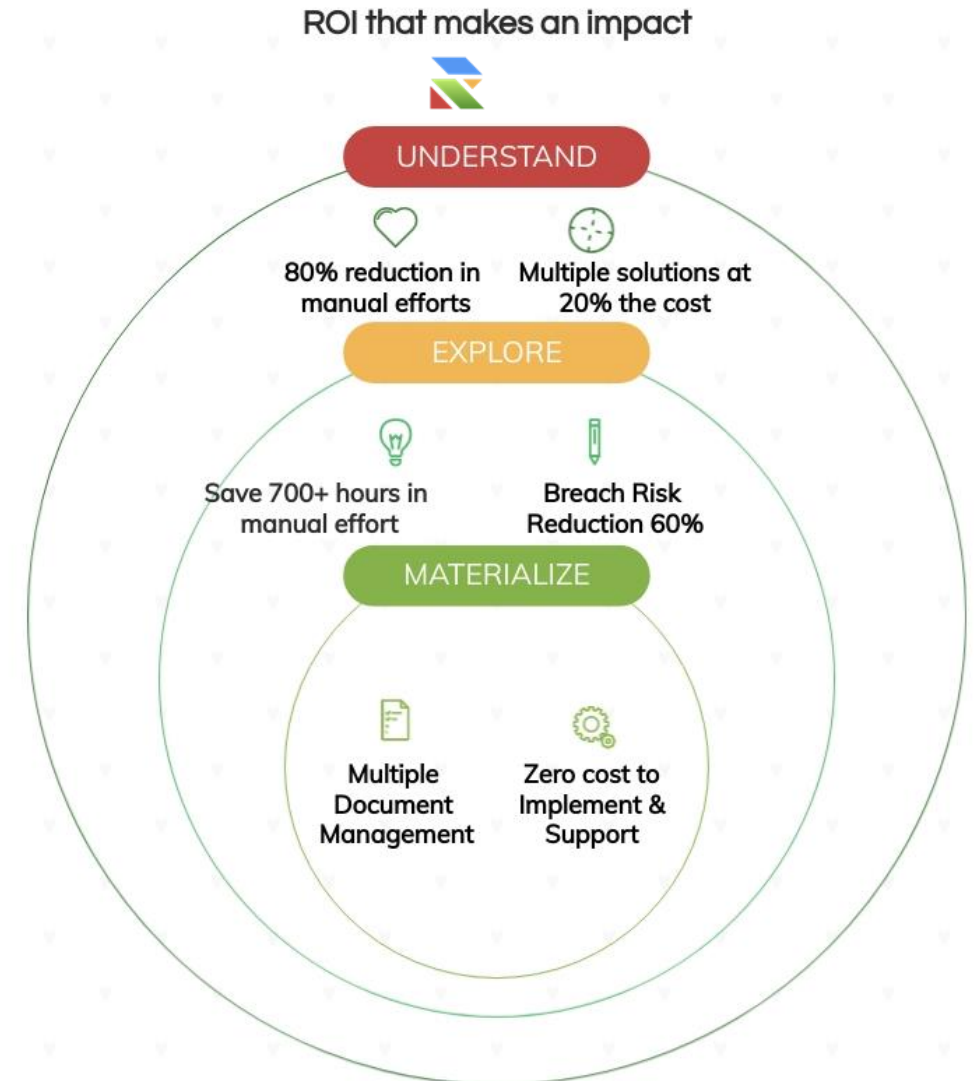


# Return On Investment

Achieving ROI that makes an impact means not only meeting financial goals but also driving significant business growth, enhancing operational efficiency, and fostering long-term sustainability.

## Key Advantages:

- 80% reduction in manual efforts
- Save 700+ hours in manual effort
- Reduce audit readiness efforts by 60%
- 70% reduction in time to compliance
- Get visibility across 100% of your controls
- 1500 % partner ROI on average in 1 year





Thank you!



Office Hours:

[\(833\) 724-7475](tel:8337247475)

M-F 9:00 am-5:30 pm EST

Please send all questions to:

[support@riskcognizance.com](mailto:support@riskcognizance.com)

[www.riskcognizance.com](http://www.riskcognizance.com)