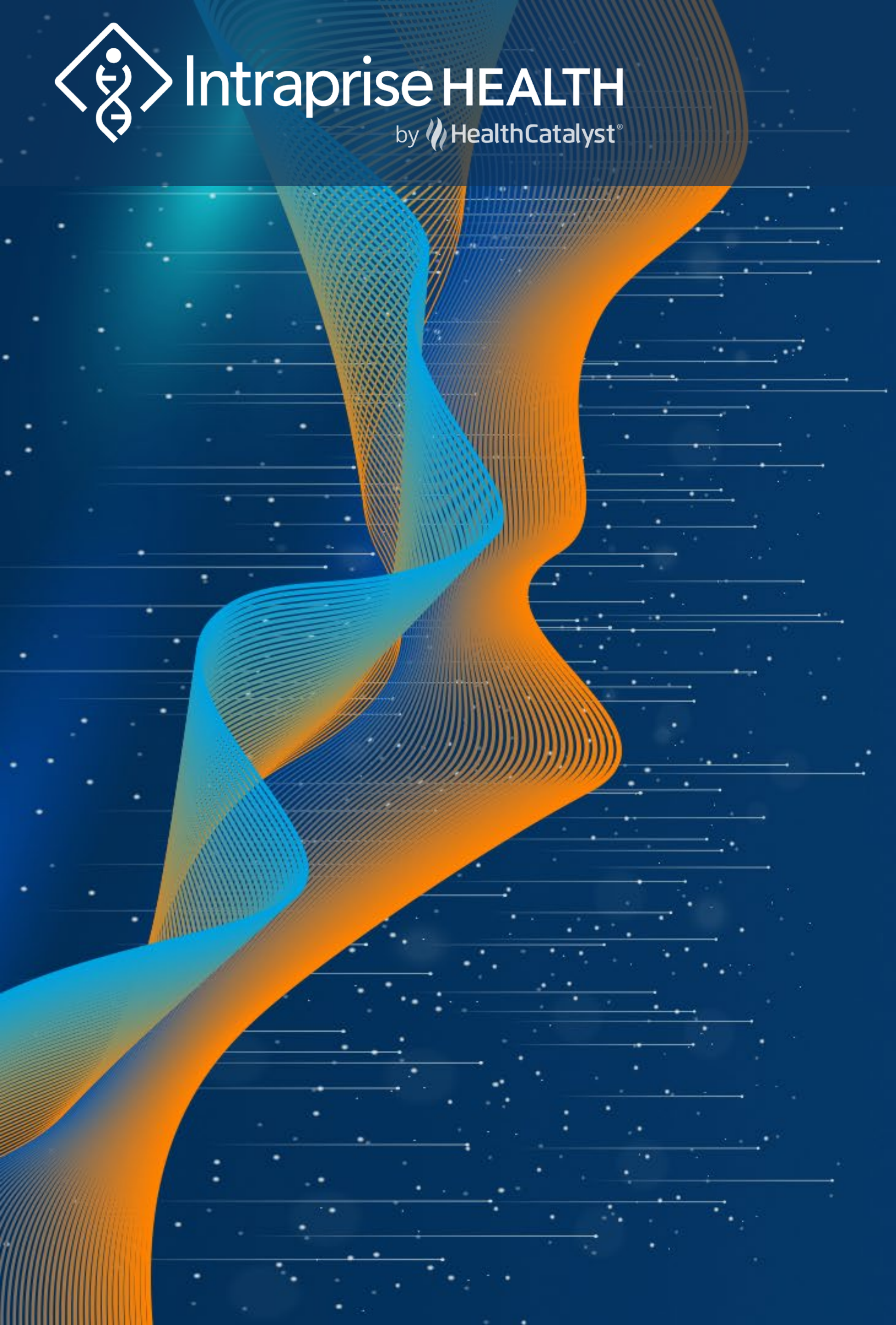
Intraprise HEALTH
by HealthCatalyst



Managing Your Risk Universe: Cybersecurity Strategies for a Secure and Scalable Future

April 2, 2025

Your Presenter

Scott Mattila, MHI, MIS

CSO and COO

Agenda

1 Enterprise Complexities

2 Building a TPRM Program

3 About Intraprise Health

4 Adopting a Cybersecurity Holistic Approach

5 Jump-Starting Your Security Program

6 Q&A

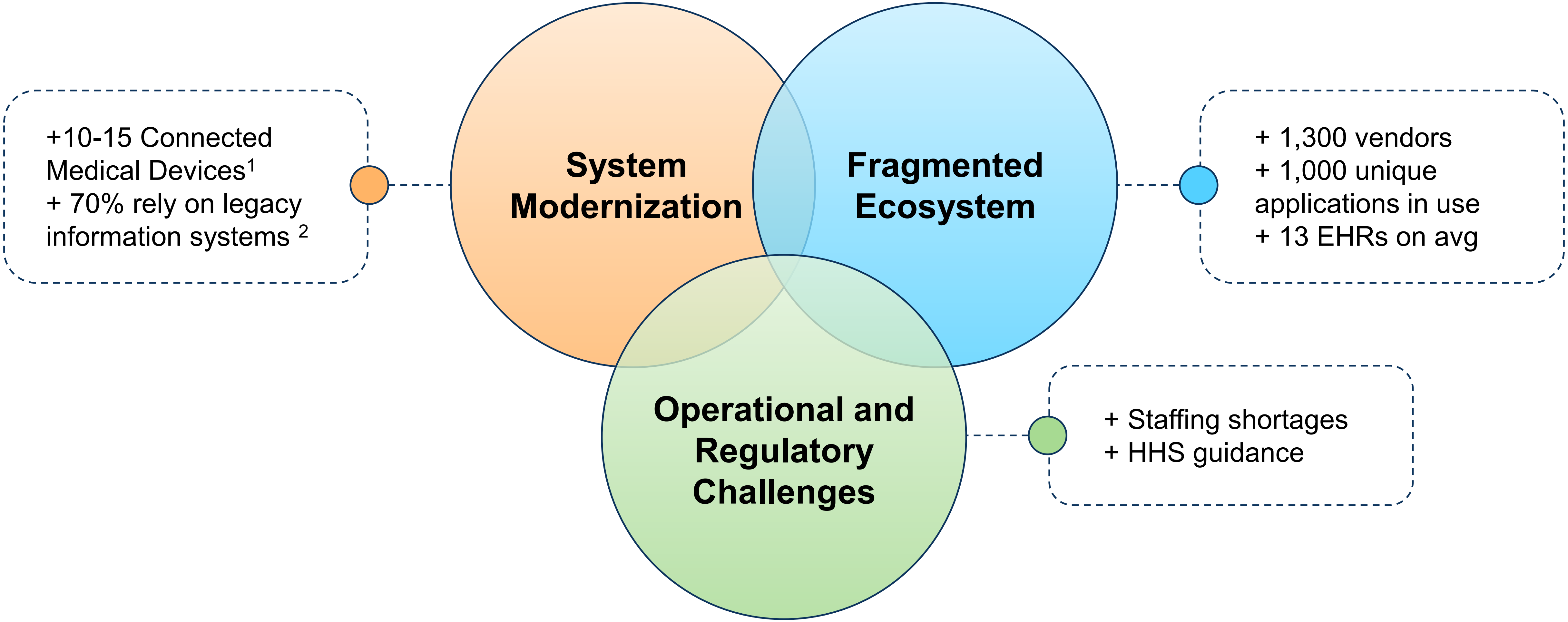
Poll Question

What are your priorities for 2025?

- A **Investigating AI** to gain care delivery efficiencies
- B **Automating your Third-Party/Vendor Exposure**
- C **Adopting a New Framework** (i.e. HITRUST and NIST CSF)
- D **Reducing Cloud Vulnerabilities**
- E **Securing Additional Investment Funding**

The Complexities of Enterprise Environments

Healthcare IoT & IOMT Security and Compliance



System Modernization

+10-15 Connected Medical Devices[1]
+ 70% rely on legacy information systems [2]

Fragmented Ecosystem

+ 1,300 vendors
+ 1,000 unique applications in use
+ 13 EHRs on avg

Operational and Regulatory Challenges

+ Staffing shortages
+ HHS guidance

Sources: (1) Digital healthcare's twin challenges: Navigating device security and patient safety, HealthData Management, September 20, 2023, (2) How best to manage, or dump, legacy healthcare IT systems, HealthcareIT News, March 2, 2023

Cybersecurity Program Outlook

2025 Security Readiness

EXECUTIVE BRIEF

Top 10 Health Technology Hazards for 2025

Expert Insights from ECRI's Device Evaluation Team

www.ecri.org

ECRI | The Most Trusted Voice in Healthcare

3

THREE

Vulnerable Technology Vendors and Cybersecurity Threats

The practice of healthcare depends heavily on the knowledge and skill of healthcare professionals, the availability and performance of in-house medical devices and systems, and—increasingly—the availability and performance of systems hosted by external (i.e., third-party) vendors. Essential tools ranging from scheduling and billing services to electronic health records and other clinical systems are frequently provided by third-party vendors.

While there are many benefits to the use of third-party tools and services, a healthcare provider's operations can be jeopardized by an event that incapacitates or degrades operations at the third-party vendor. In several high-profile cases, instances of unauthorized access, service disruptions, or other adverse cybersecurity events that impacted a vendor had far-reaching implications for patient care—the 2024 attack on Change Healthcare and the resulting nationwide disruption to pharmacy and billing services being one example.

Such incidents can leave healthcare providers without access to critical services, reliable data, or effective communications channels with their partners. Any of those eventualities can put patients in harm's way, delaying, preventing, or degrading care and adversely affecting patient outcomes.

Measures that can help a healthcare organization mitigate third-party risks include thoroughly vetting vendors at the start of the service acquisition process, building in redundancy, conducting incident response testing, and developing recovery procedures.

Further, ECRI encourages government bodies, regulatory agencies, and others in industry to move away from "punish but not protect" approaches to cybersecurity challenges and third-party risks and toward fostering a collective approach to cybercrime and vendor risk.

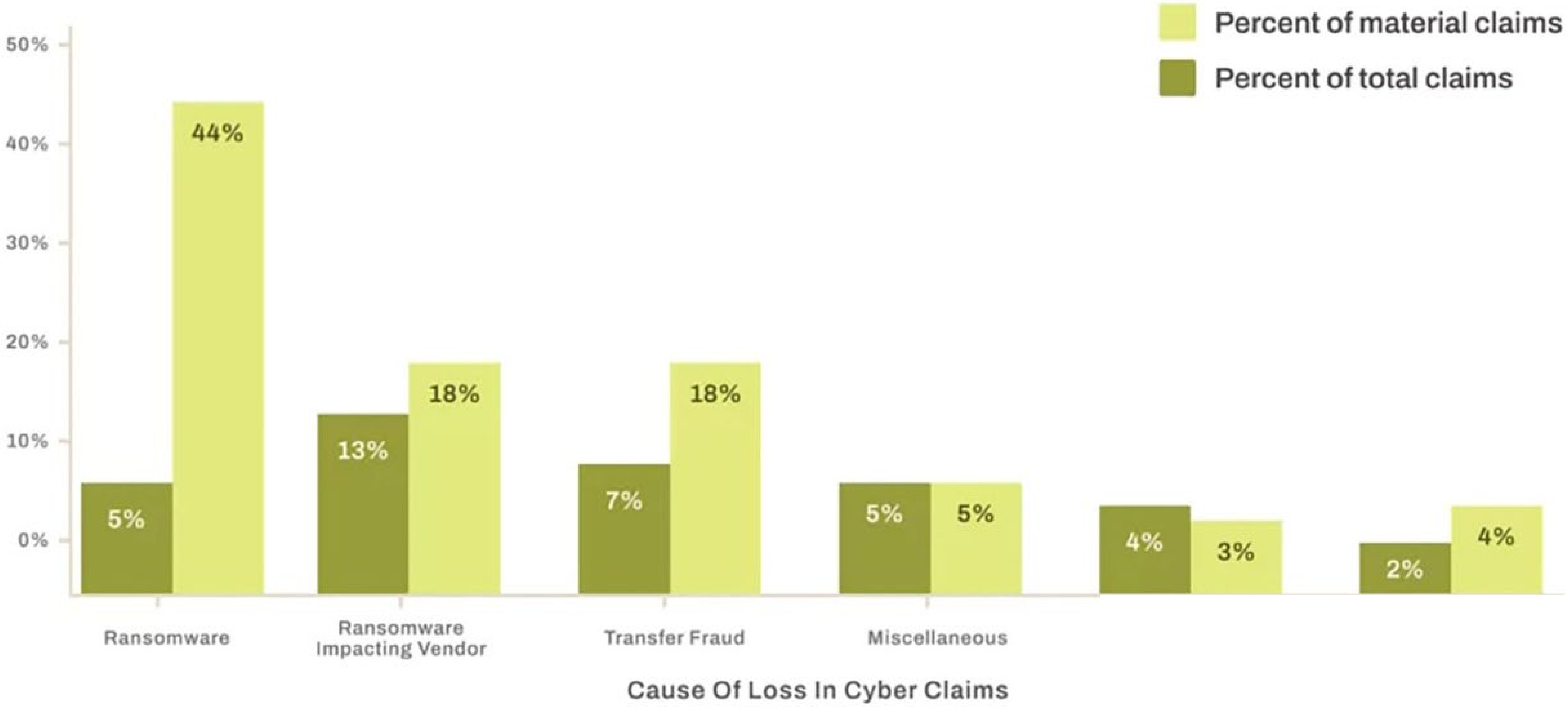
> A healthcare provider's operations can be jeopardized by a cybersecurity event that incapacitates or degrades operations at a third-party vendor.

Top 10 Health Technology Hazards for 2025 | EXECUTIVE BRIEF

The 2025 List | DeviceEvaluation@ecri.org | 8

Third-Party Risk Top Cybersecurity Claims

Ransomware – The largest share of insurance claims



Source: Third-Party Risk Tops Cybersecurity Claims, DarkReading.com, February 28, 2025

The Cost of a Breach

Third-Party Partner Risks

35%

Third-Party Attacks

against healthcare were caused by vendors[1]

40%

Signed Contracts

are finalized with third-party vendors without conducting a risk assessment[2]

23%

Mortality Rate

of attacked healthcare organizations experience increased mortality rates[3]

Sources: (1) Healthcare leads in third-party data breaches, says new report, Healthcare IT News, June 25, 2024, (2) Ransomware Attacks in healthcare: Stats and Recommendations, PhoenixNAP, March 16, 2023, (3) Second Annual Ponemon Institute Report Finds that Two-Thirds of Healthcare Organizations Surveyed Experienced Disruption to Patient Care Due to Cyber Attacks, October 11, 2023

Latest Trends

Landscape and Cyber Opportunities

Massive shortage in cybersecurity talent. Expected job growth market of 33% over the next 10 years

Under threat, short staff, limited leadership buy-in, and lack of funding

Cybercrime is expected to reach $10.5 trillion annually in 2025

The healthcare sector is hit more than any other industry, accounting for 23% of all data breaches

Regulation changes, vendor risks, and assessment fatigue are leading to increased threats to business operations

Building a Third-Party Risk Program

Getting Started with BluePrint Protect™

Poll Question

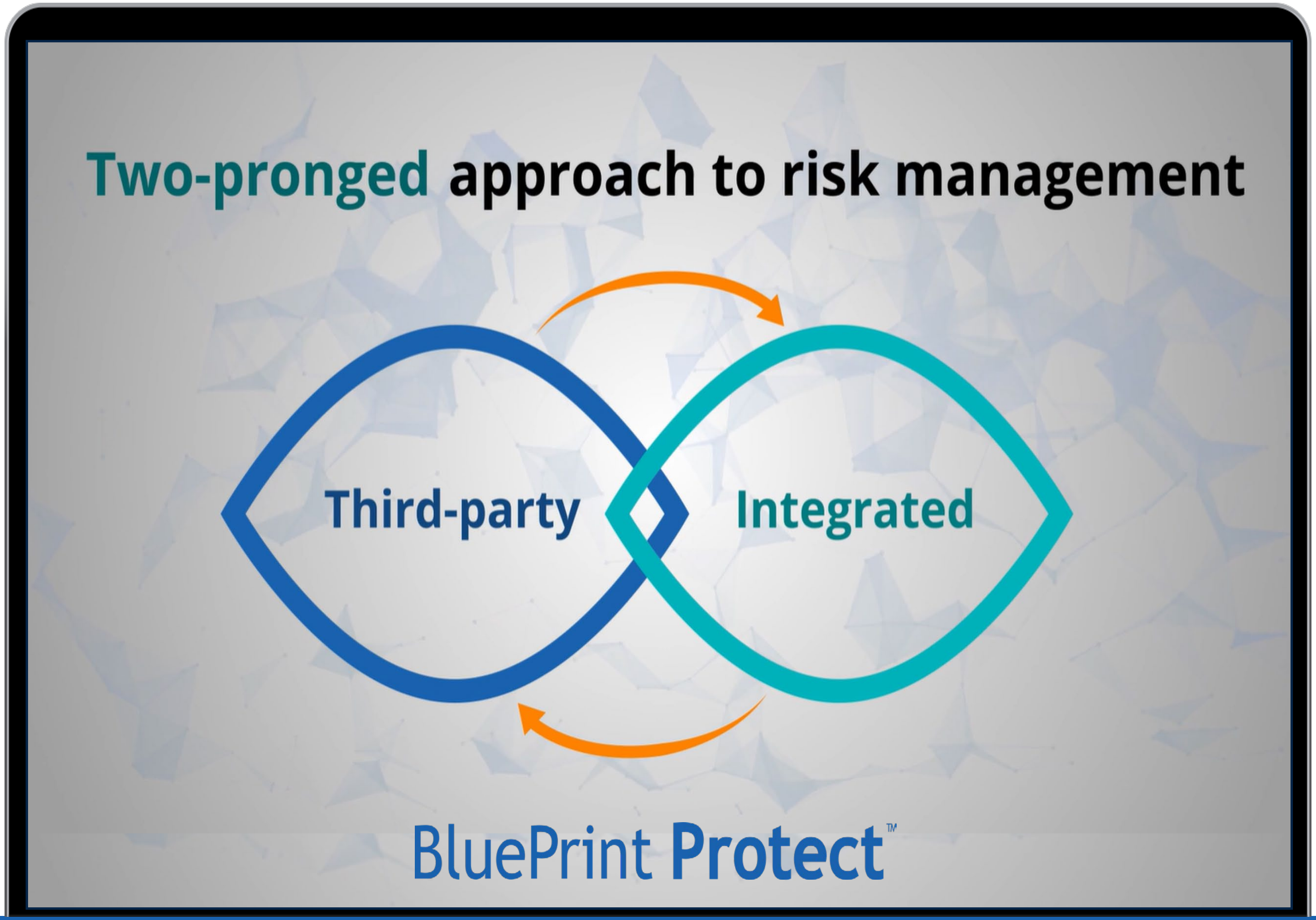
Which methods is your organization using to manage third-party risk?

- A **Manual Solutions** (i.e. Spreadsheets, paper)
- B **A Governance, Risk, and Compliance (GRC) Platform**
- C **A Third-Party Risk Management Platform**
- D **Consultants are Managing our Vendor Risk Program**
- E **A Mixture of the Above Solutions**

What is BluePrint Protect™?

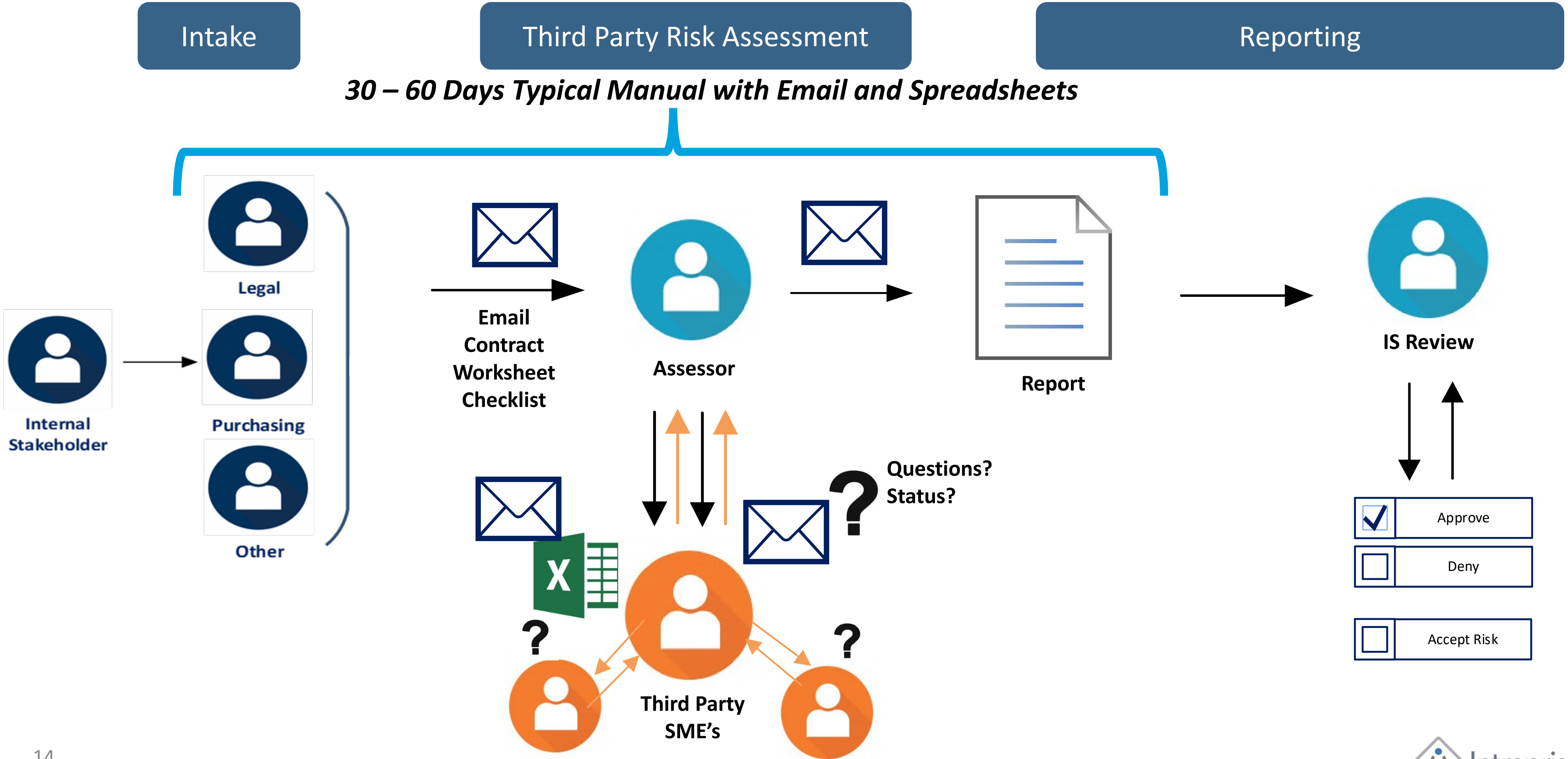
A Holistic Approach to Risk Management

- Enables seamless risk management and collaboration through a unified, actionable dashboard
- Delivers a unified risk view by integrating internal and third-party risk, and compliance assessments
- Seamless integration with existing assessments and reports
- Provides actionable reports to quantify cyber risks for insurance auditors and providers



Two-pronged approach to risk management

Common Manual Process in Health Systems



BluePrint Protect™ Third Party Risk Management

Automated Assessment Workflow with Validation

< 10 Days Typical with Workflow Automation & AI Protect Assistant

IS Team

Third Party

Assessor

BluePrint **Protect**™

Assessment Request

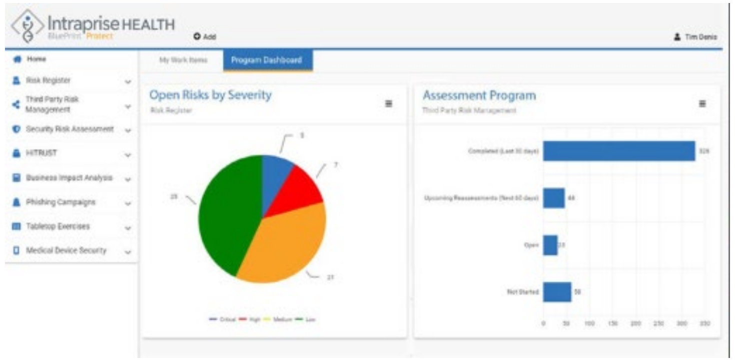
Assessment Response

75% Faster!

Protect Assistant

Assessment Review

AI Powered Controls & Evidence Evaluation



Real-Time Status Tracking

Protect Assistant

Risk Rating & Reporting

☑ Approve

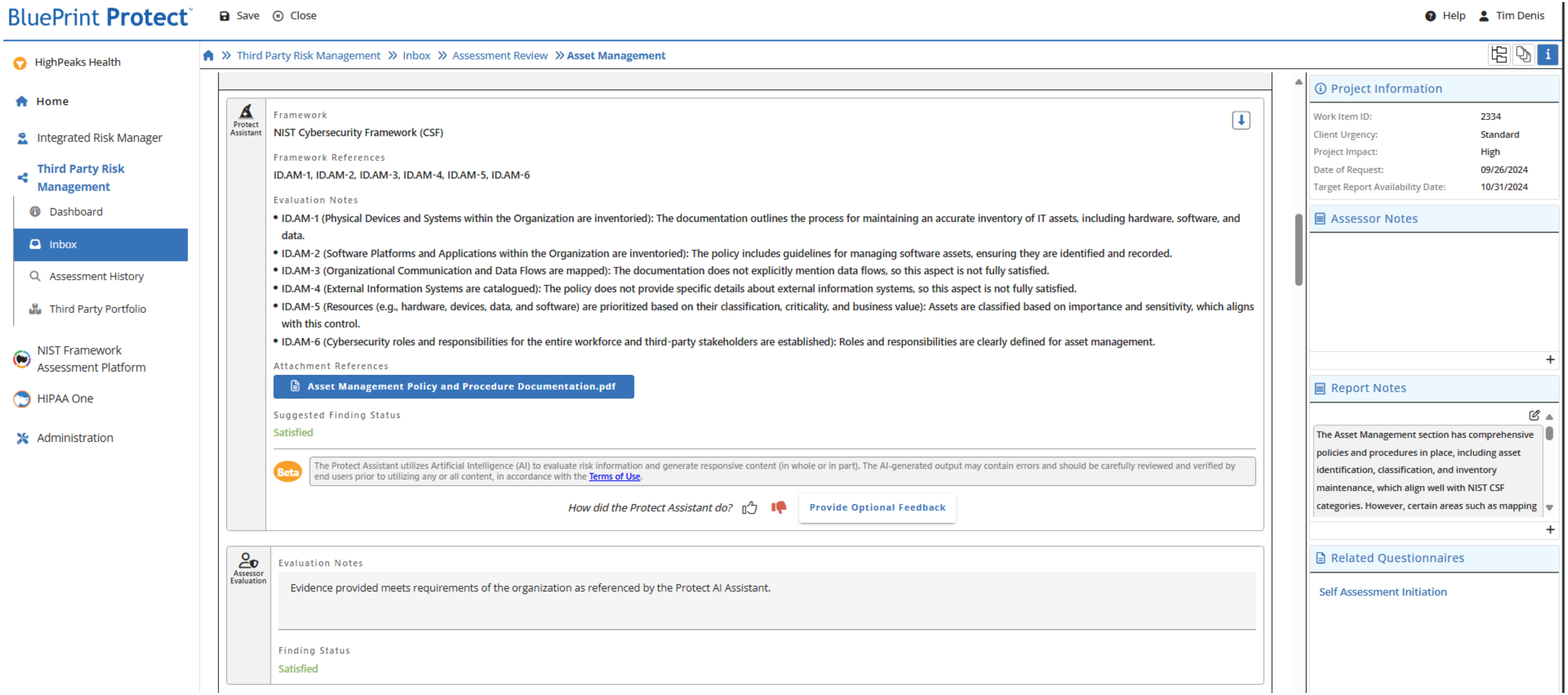
□ Deny

□ Accept Risk

Use Case:
Automation and Integration

Assessment Management

New Additions - Organizational and Application/System Management Assessments



Framework

NIST Cybersecurity Framework (CSF)

Framework References

ID.AM-1, ID.AM-2, ID.AM-3, ID.AM-4, ID.AM-5, ID.AM-6

Evaluation Notes

- ID.AM-1 (Physical Devices and Systems within the Organization are inventoried): The documentation outlines the process for maintaining an accurate inventory of IT assets, including hardware, software, and data.
- ID.AM-2 (Software Platforms and Applications within the Organization are inventoried): The policy includes guidelines for managing software assets, ensuring they are identified and recorded.
- ID.AM-3 (Organizational Communication and Data Flows are mapped): The documentation does not explicitly mention data flows, so this aspect is not fully satisfied.
- ID.AM-4 (External Information Systems are catalogued): The policy does not provide specific details about external information systems, so this aspect is not fully satisfied.
- ID.AM-5 (Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value): Assets are classified based on importance and sensitivity, which aligns with this control.
- ID.AM-6 (Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders are established): Roles and responsibilities are clearly defined for asset management.

Attachment References

Asset Management Policy and Procedure Documentation.pdf

Suggested Finding Status

Satisfied

Beta The Protect Assistant utilizes Artificial Intelligence (AI) to evaluate risk information and generate responsive content (in whole or in part). The AI-generated output may contain errors and should be carefully reviewed and verified by end users prior to utilizing any or all content, in accordance with the Terms of Use.

How did the Protect Assistant do? Provide Optional Feedback

Evaluation Notes

Evidence provided meets requirements of the organization as referenced by the Protect AI Assistant.

Finding Status

Satisfied

Project Information

Work Item ID:	2334
Client Urgency:	Standard
Project Impact:	High
Date of Request:	09/26/2024
Target Report Availability Date:	10/31/2024

Assessor Notes

Report Notes

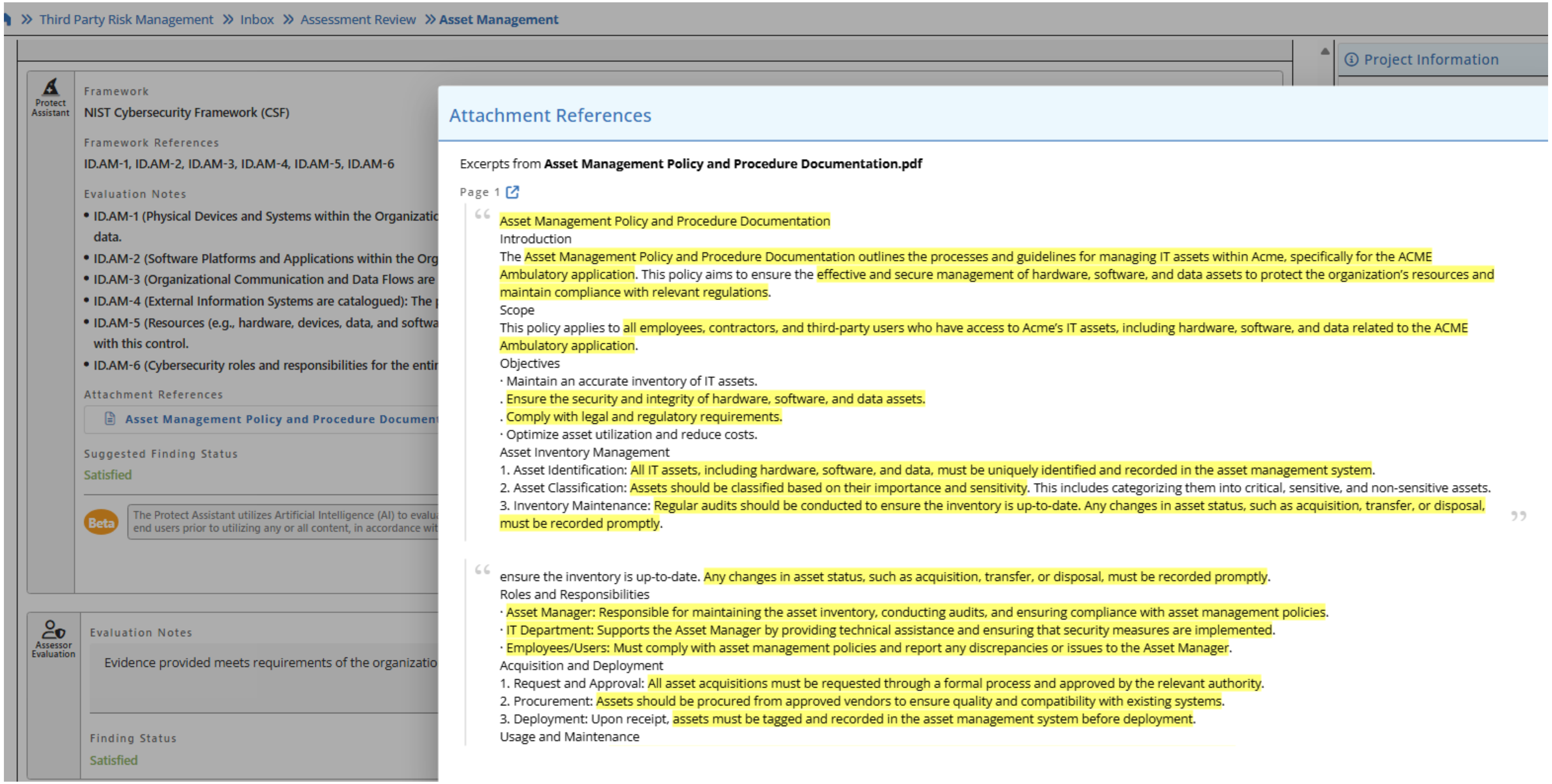
The Asset Management section has comprehensive policies and procedures in place, including asset identification, classification, and inventory maintenance, which align well with NIST CSF categories. However, certain areas such as mapping

Related Questionnaires

Self Assessment Initiation

Assessment Management

Simplified Policy and Procedure workflows



Third Party Risk Management » Inbox » Assessment Review » Asset Management
Project Information
Protect Assistant
Assessor Evaluation
Beta

Framework
NIST Cybersecurity Framework (CSF)

Framework References
ID.AM-1, ID.AM-2, ID.AM-3, ID.AM-4, ID.AM-5, ID.AM-6

Evaluation Notes

- ID.AM-1 (Physical Devices and Systems within the Organizatic
data.
- ID.AM-2 (Software Platforms and Applications within the Org
- ID.AM-3 (Organizational Communication and Data Flows are
- ID.AM-4 (External Information Systems are catalogued): The
- ID.AM-5 (Resources (e.g., hardware, devices, data, and softwa
with this control.
- ID.AM-6 (Cybersecurity roles and responsibilities for the entir

Attachment References
Asset Management Policy and Procedure Documen

Suggested Finding Status
Satisfied

The Protect Assistant utilizes Artificial Intelligence (AI) to evalu
end users prior to utilizing any or all content, in accordance wi

Evaluation Notes
Evidence provided meets requirements of the organizatio

Finding Status
Satisfied

Attachment References

Excerpts from **Asset Management Policy and Procedure Documentation.pdf**

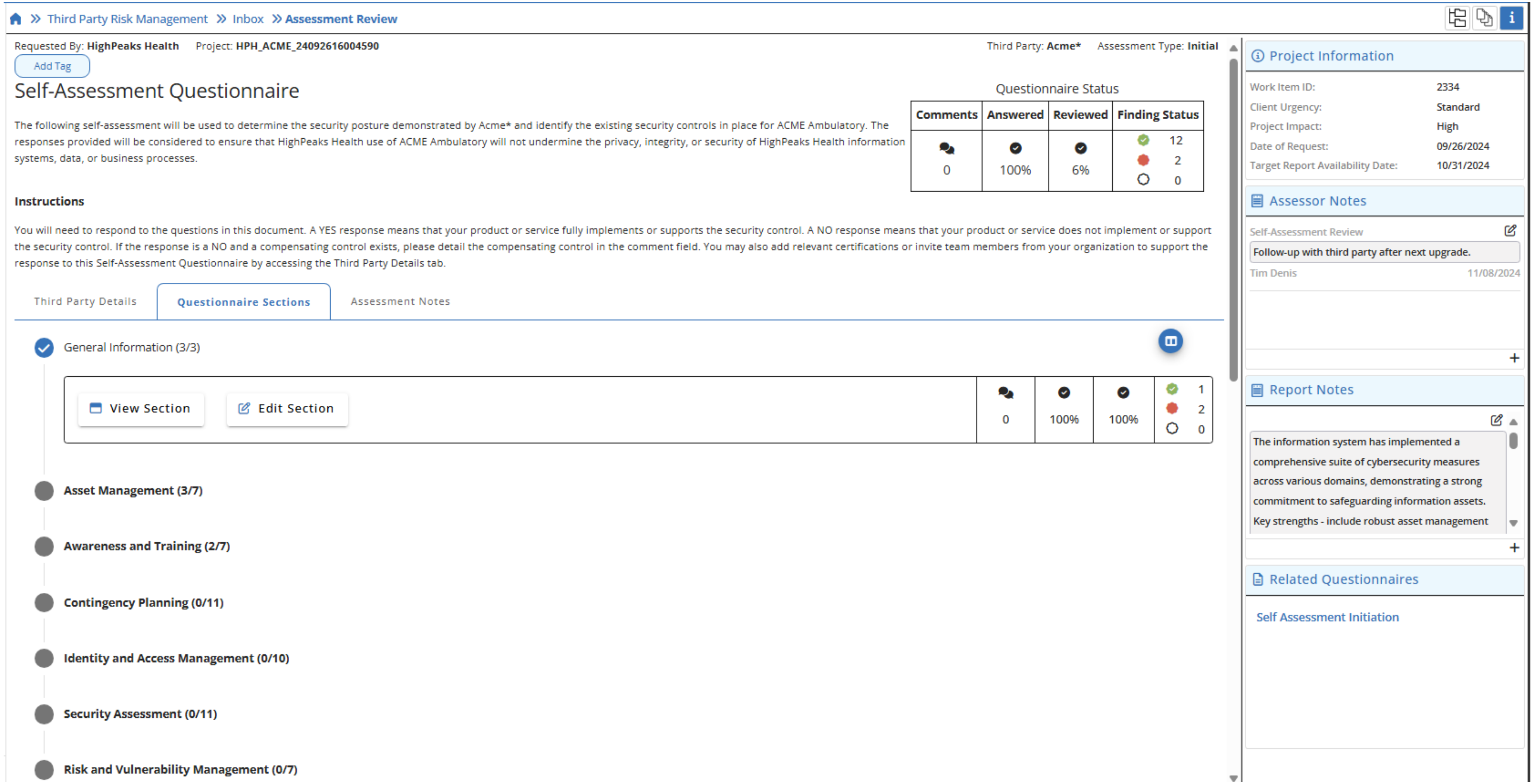
Page 1

> Asset Management Policy and Procedure Documentation
> Introduction
> The Asset Management Policy and Procedure Documentation outlines the processes and guidelines for managing IT assets within Acme, specifically for the ACME Ambulatory application. This policy aims to ensure the effective and secure management of hardware, software, and data assets to protect the organization’s resources and maintain compliance with relevant regulations.
> Scope
> This policy applies to all employees, contractors, and third-party users who have access to Acme’s IT assets, including hardware, software, and data related to the ACME Ambulatory application.
> Objectives
> · Maintain an accurate inventory of IT assets.
> . Ensure the security and integrity of hardware, software, and data assets.
> . Comply with legal and regulatory requirements.
> · Optimize asset utilization and reduce costs.
> Asset Inventory Management
> 1. Asset Identification: All IT assets, including hardware, software, and data, must be uniquely identified and recorded in the asset management system.
> 2. Asset Classification: Assets should be classified based on their importance and sensitivity. This includes categorizing them into critical, sensitive, and non-sensitive assets.
> 3. Inventory Maintenance: Regular audits should be conducted to ensure the inventory is up-to-date. Any changes in asset status, such as acquisition, transfer, or disposal, must be recorded promptly.

> ensure the inventory is up-to-date. Any changes in asset status, such as acquisition, transfer, or disposal, must be recorded promptly.
> Roles and Responsibilities
> · Asset Manager: Responsible for maintaining the asset inventory, conducting audits, and ensuring compliance with asset management policies.
> · IT Department: Supports the Asset Manager by providing technical assistance and ensuring that security measures are implemented.
> · Employees/Users: Must comply with asset management policies and report any discrepancies or issues to the Asset Manager.
> Acquisition and Deployment
> 1. Request and Approval: All asset acquisitions must be requested through a formal process and approved by the relevant authority.
> 2. Procurement: Assets should be procured from approved vendors to ensure quality and compatibility with existing systems.
> 3. Deployment: Upon receipt, assets must be tagged and recorded in the asset management system before deployment.
> Usage and Maintenance

Vendor Questionnaires

Reduce the time and effort to evaluate third-party partners



Requested By: **HighPeaks Health** Project: **HPH_ACME_24092616004590** Third Party: **Acme*** Assessment Type: **Initial**

Self-Assessment Questionnaire

The following self-assessment will be used to determine the security posture demonstrated by Acme* and identify the existing security controls in place for ACME Ambulatory. The responses provided will be considered to ensure that HighPeaks Health use of ACME Ambulatory will not undermine the privacy, integrity, or security of HighPeaks Health information systems, data, or business processes.

Questionnaire Status

Comments	Answered	Reviewed	Finding Status
0	100%	6%	🟢 12 🔴 2 ○ 0

Instructions

You will need to respond to the questions in this document. A YES response means that your product or service fully implements or supports the security control. A NO response means that your product or service does not implement or support the security control. If the response is a NO and a compensating control exists, please detail the compensating control in the comment field. You may also add relevant certifications or invite team members from your organization to support the response to this Self-Assessment Questionnaire by accessing the Third Party Details tab.

✓ General Information (3/3)

Comments	Answered	Reviewed	Finding Status
0	100%	100%	🟢 1 🔴 2 ○ 0

● **Asset Management (3/7)**

● **Awareness and Training (2/7)**

● **Contingency Planning (0/11)**

● **Identity and Access Management (0/10)**

● **Security Assessment (0/11)**

● **Risk and Vulnerability Management (0/7)**

Project Information

Work Item ID:	2334
Client Urgency:	Standard
Project Impact:	High
Date of Request:	09/26/2024
Target Report Availability Date:	10/31/2024

Assessor Notes

Self-Assessment Review

Follow-up with third party after next upgrade.

Tim Denis 11/08/2024

Report Notes

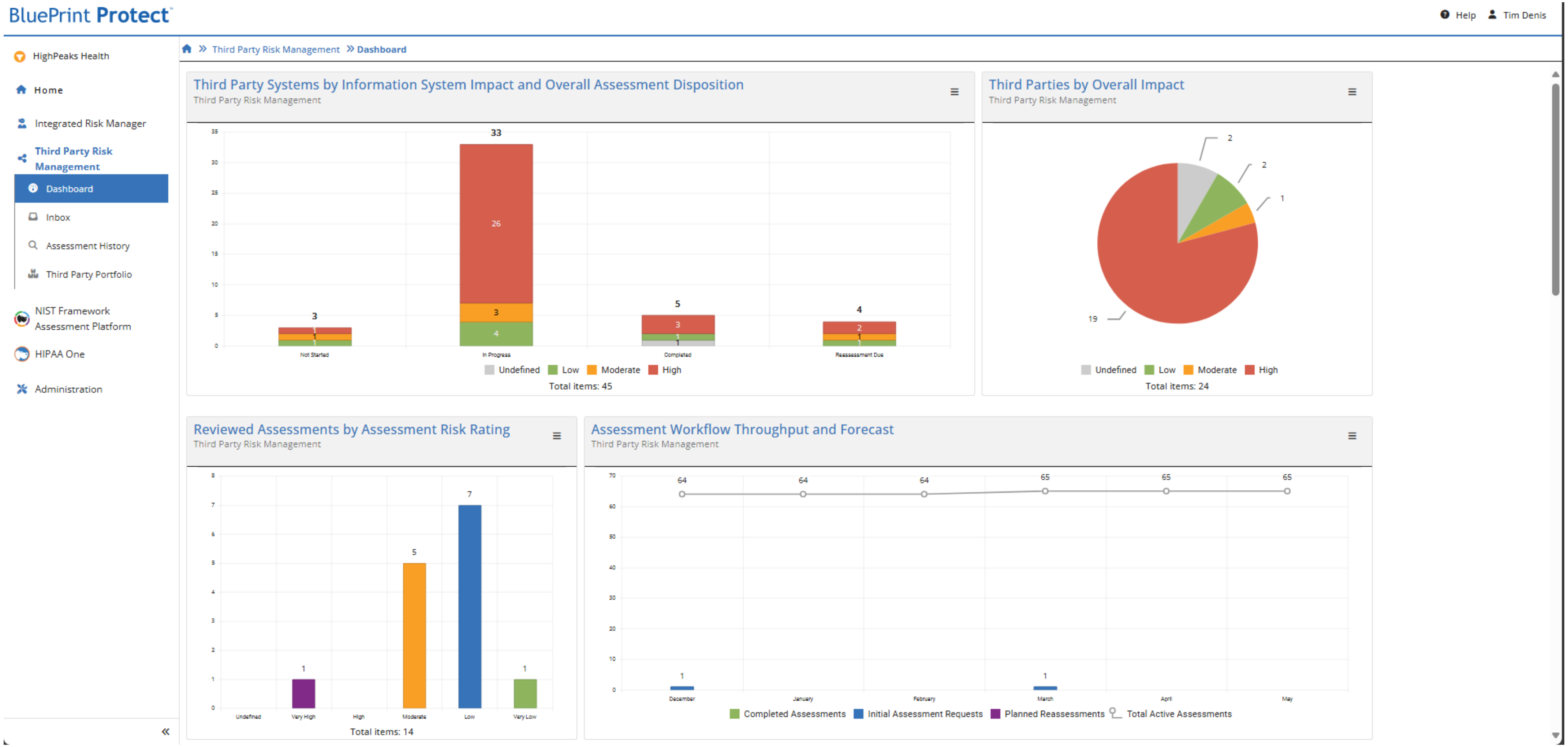
The information system has implemented a comprehensive suite of cybersecurity measures across various domains, demonstrating a strong commitment to safeguarding information assets. Key strengths - include robust asset management

Related Questionnaires

Self Assessment Initiation

Third-Party Risk Management

TPRM Dashboard with risk scoring and organization impact insights



Third Party Systems by Information System Impact and Overall Assessment Disposition

Third Party Risk Management

Third Parties by Overall Impact

Third Party Risk Management

Reviewed Assessments by Assessment Risk Rating

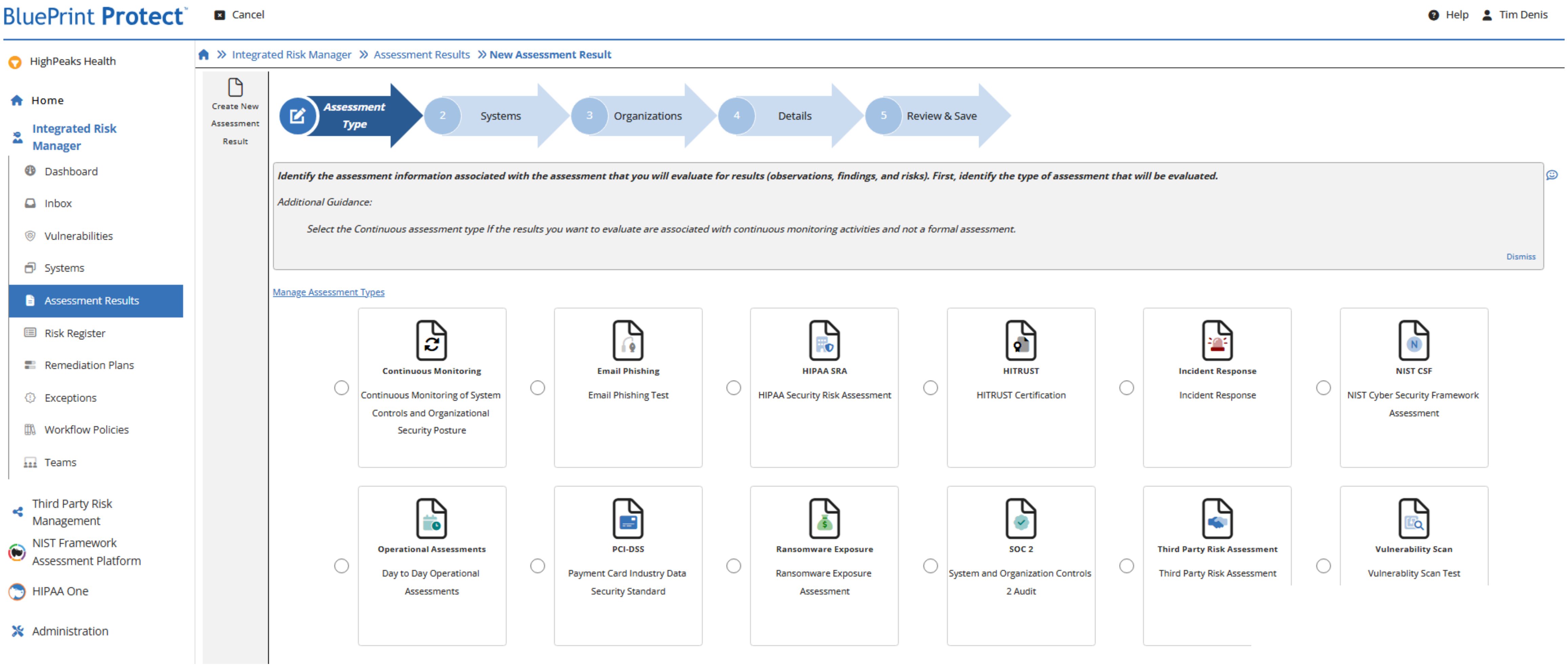
Third Party Risk Management

Assessment Workflow Throughput and Forecast

Third Party Risk Management

Holistic Risk View

Real-time risk management to strengthen program effectiveness and security



Identify the assessment information associated with the assessment that you will evaluate for results (observations, findings, and risks). First, identify the type of assessment that will be evaluated.

Additional Guidance:

Select the Continuous assessment type If the results you want to evaluate are associated with continuous monitoring activities and not a formal assessment.

○ **Continuous Monitoring** Continuous Monitoring of System Controls and Organizational Security Posture

○ **Email Phishing** Email Phishing Test

○ **HIPAA SRA** HIPAA Security Risk Assessment

○ **HITRUST** HITRUST Certification

○ **Incident Response** Incident Response

○ **NIST CSF** NIST Cyber Security Framework Assessment

○ **Operational Assessments** Day to Day Operational Assessments

○ **PCI-DSS** Payment Card Industry Data Security Standard

○ **Ransomware Exposure** Ransomware Exposure Assessment

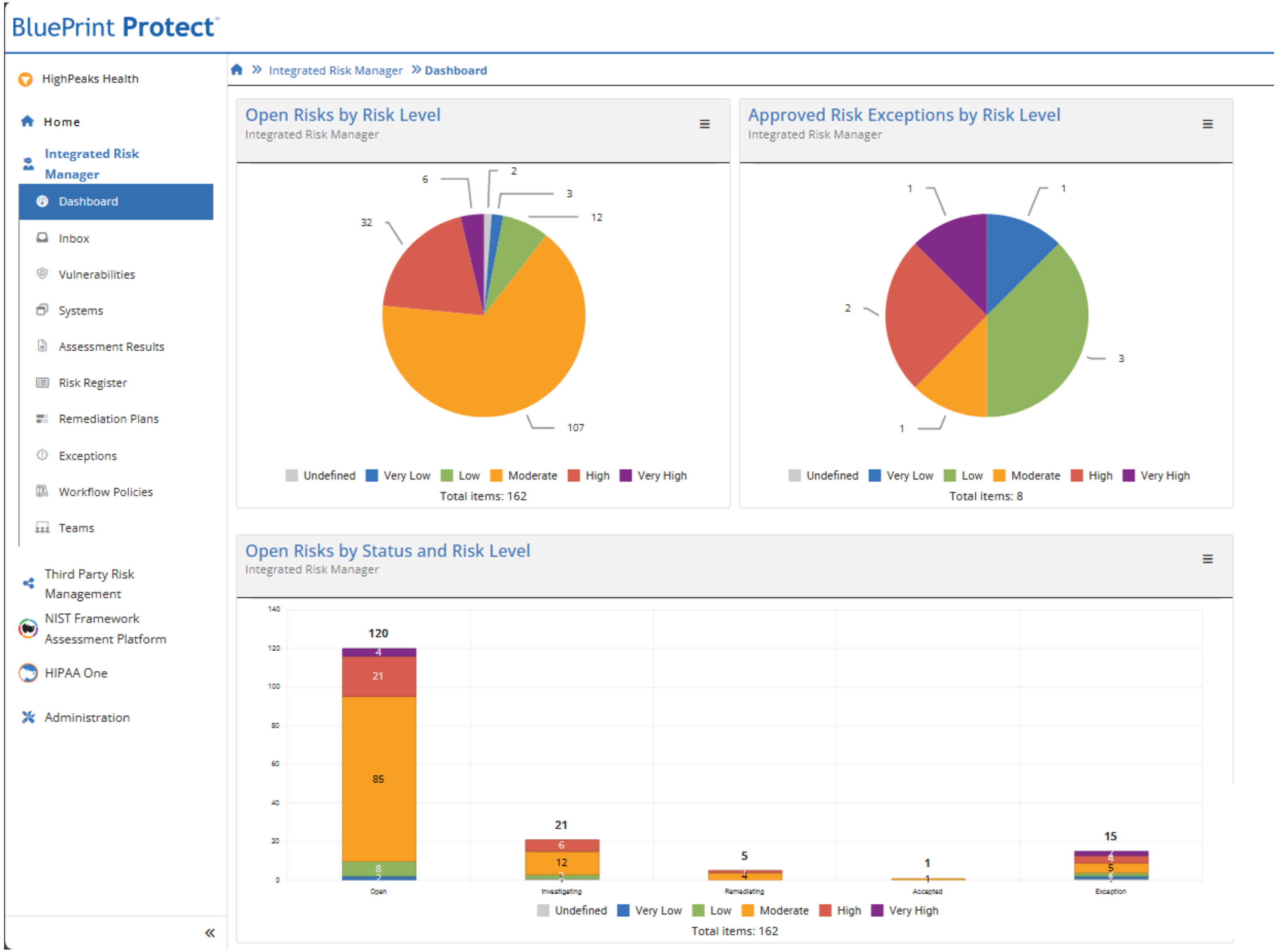
○ **SOC 2** System and Organization Controls 2 Audit

○ **Third Party Risk Assessment** Third Party Risk Assessment

○ **Vulnerability Scan** Vulnerablity Scan Test

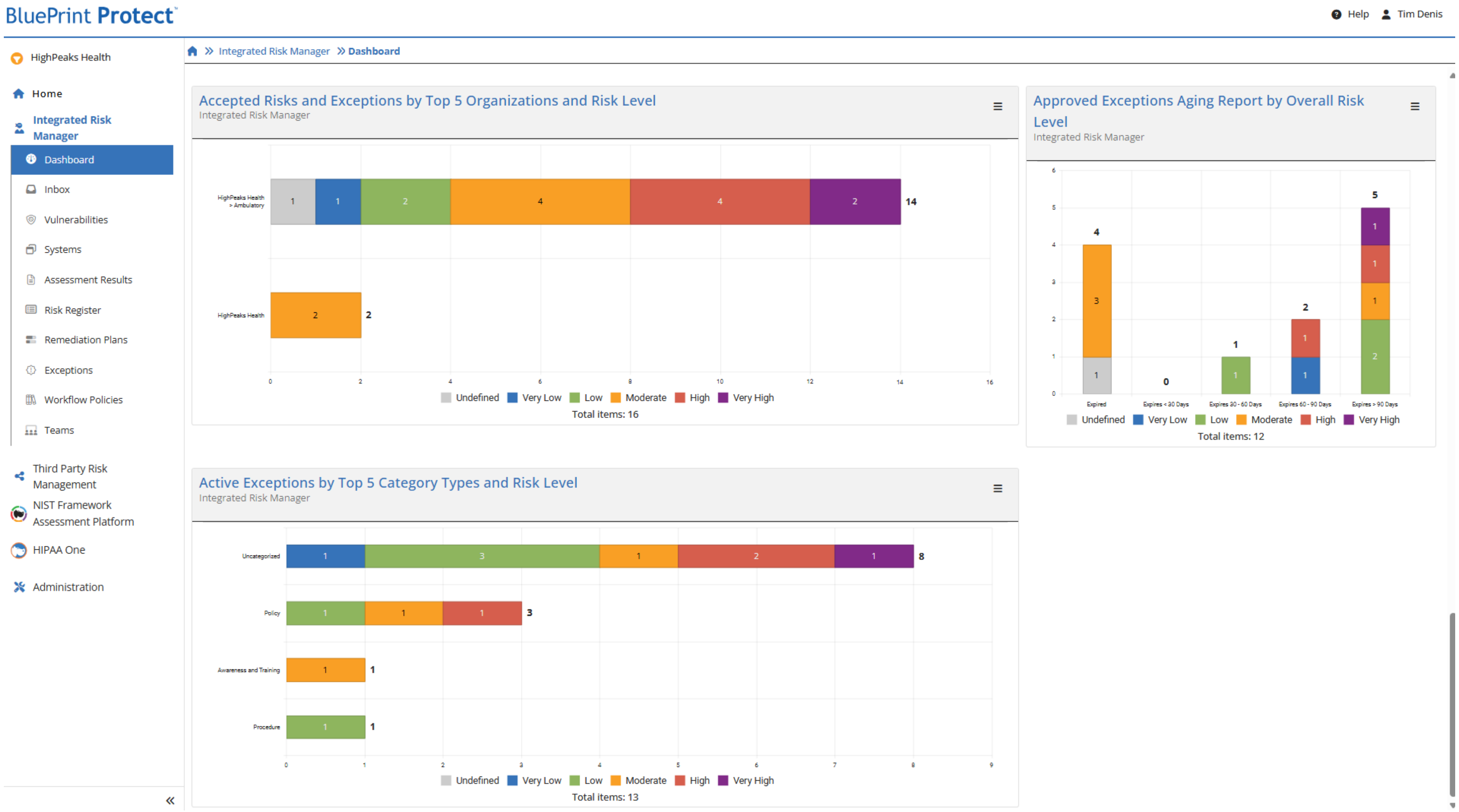
Open Risks and Exceptions

360-degree risk insights for proactive planning and remediation



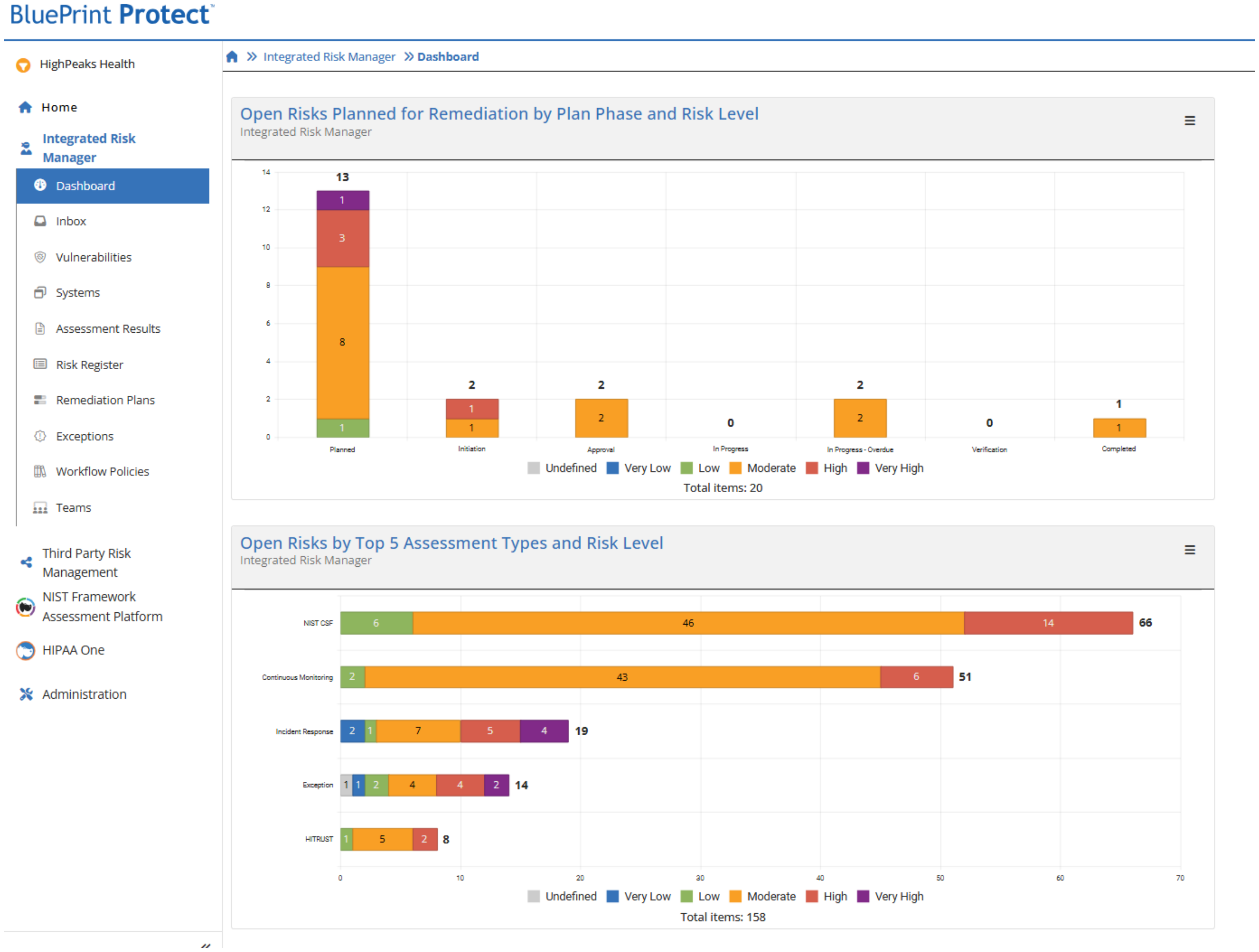
Accepted Risks and Exceptions

Centralized risk acceptance monitoring



Remediation Planning

Monitor all assessments to enhance risk posture continuously



Open Risks Planned for Remediation by Plan Phase and Risk Level

Integrated Risk Manager

Total items: 20

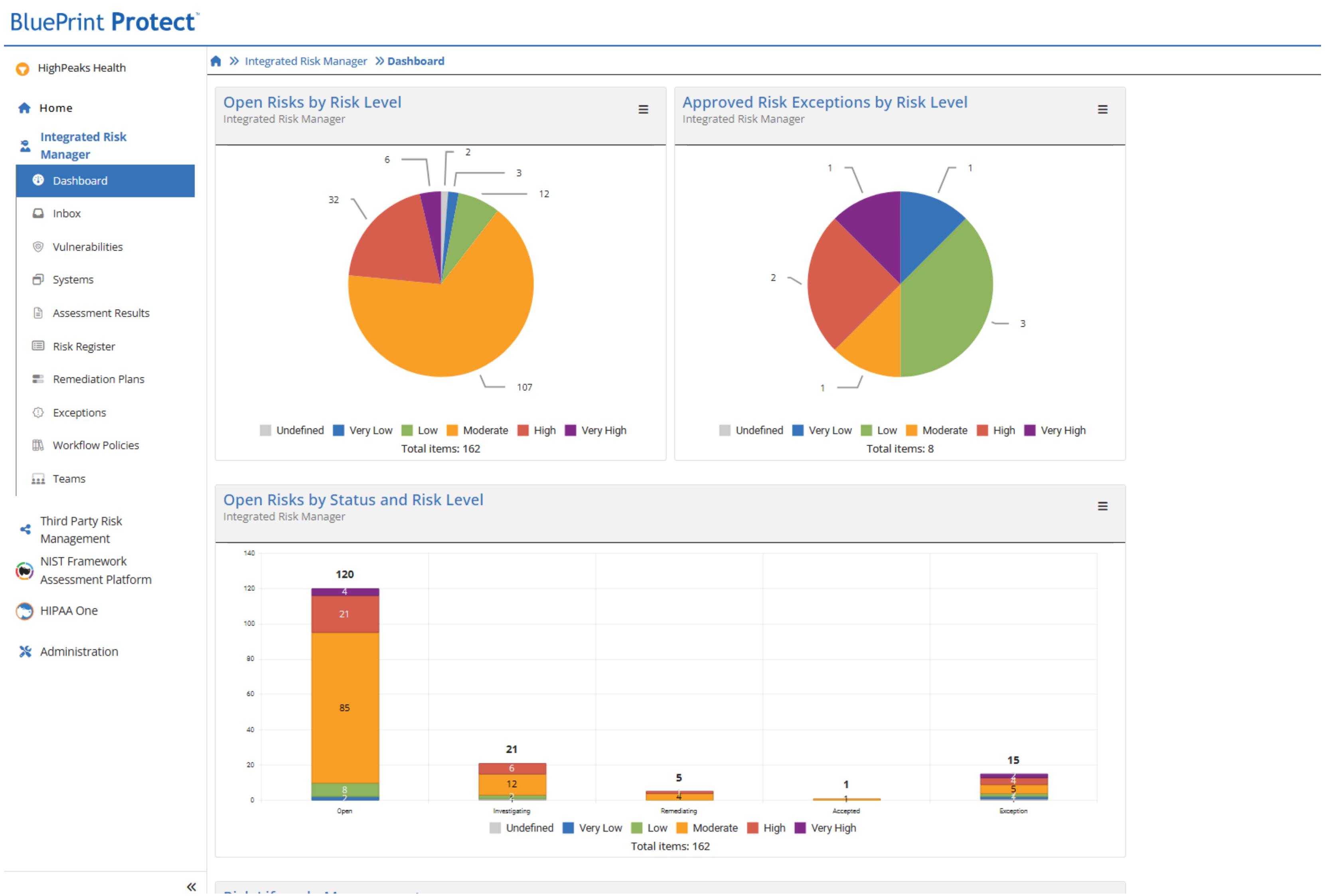
Open Risks by Top 5 Assessment Types and Risk Level

Integrated Risk Manager

Total items: 158

Exception Management

Centralize, analyze, and minimize accepted risks



Who is Intraprise Health?

About Intraprise Health

Arkansas

CENTENE Corporation

Frederick Health

Stony Brook University

UIC UI Health

Valley Health System

UNC HEALTH

Domain Experience

KLAS RESEARCH
CUSTOMER RATED
Emerging Company Spotlight

TOP HEALTHCARE SOLUTIONS VENDOR

IMPARTIAL ACCURATE BLACK BOOK UNBIASED SOURCE

Industry Recognition

We're an industry-leading, tech-enabled cybersecurity services provider offering an end-to-end cybersecurity risk management platform and services to protect from cyberattacks and manage follow-on liability in the event of an incident.

We adhere to compliance frameworks, identify cybersecurity vulnerabilities, and assess third-party risks. Intraprise Health removes blind spots—a HITRUST assessor since 2011, the fifth to achieve this distinction.

Certified Team of Healthcare Security & Privacy Experts

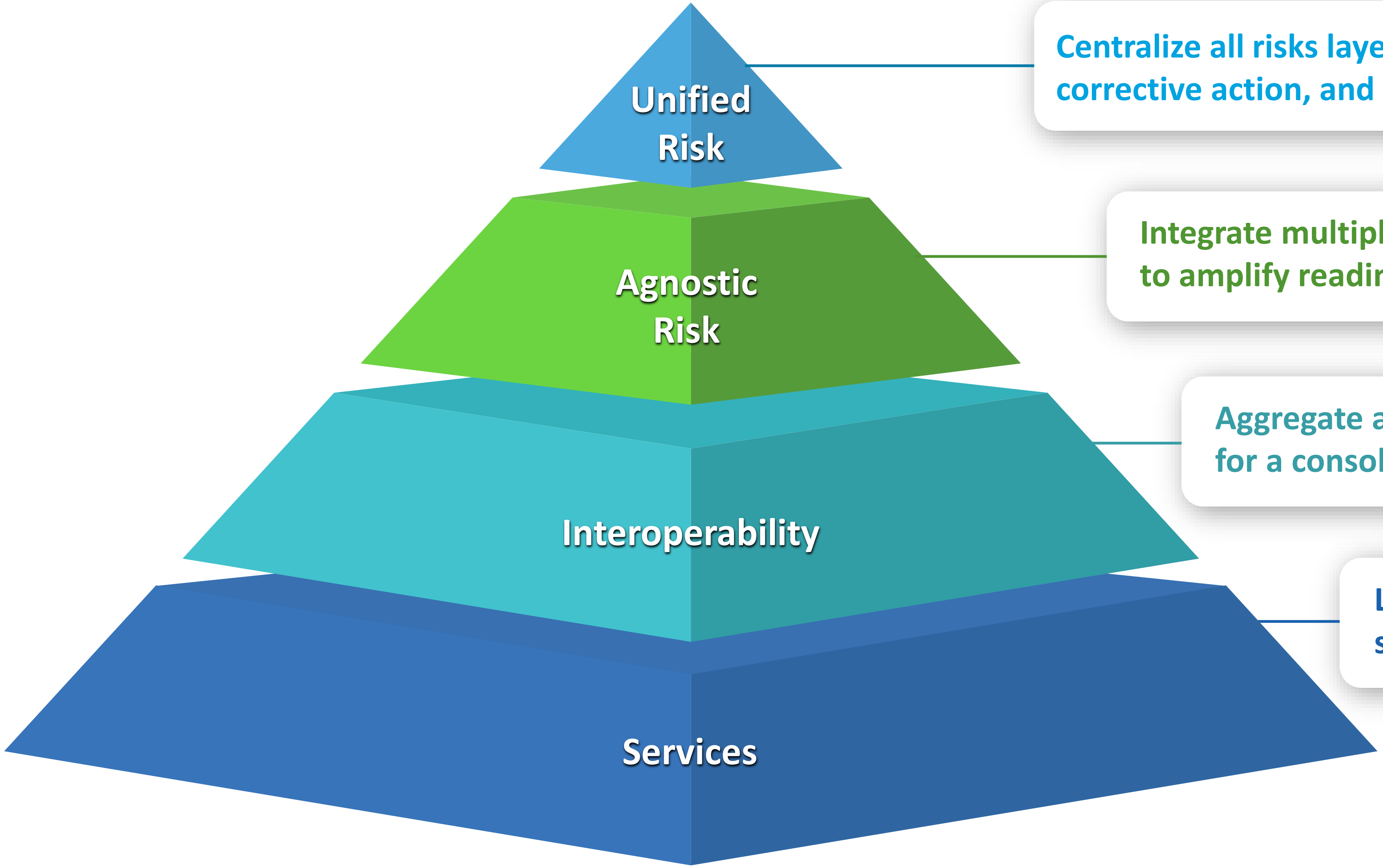
Industry Leading Software & Services – Constant Innovation

10+

Proven Leadership Team & Subject Matter Experts

Unifying Risk Pyramid

Building Blocks for Cybersecurity Resilience



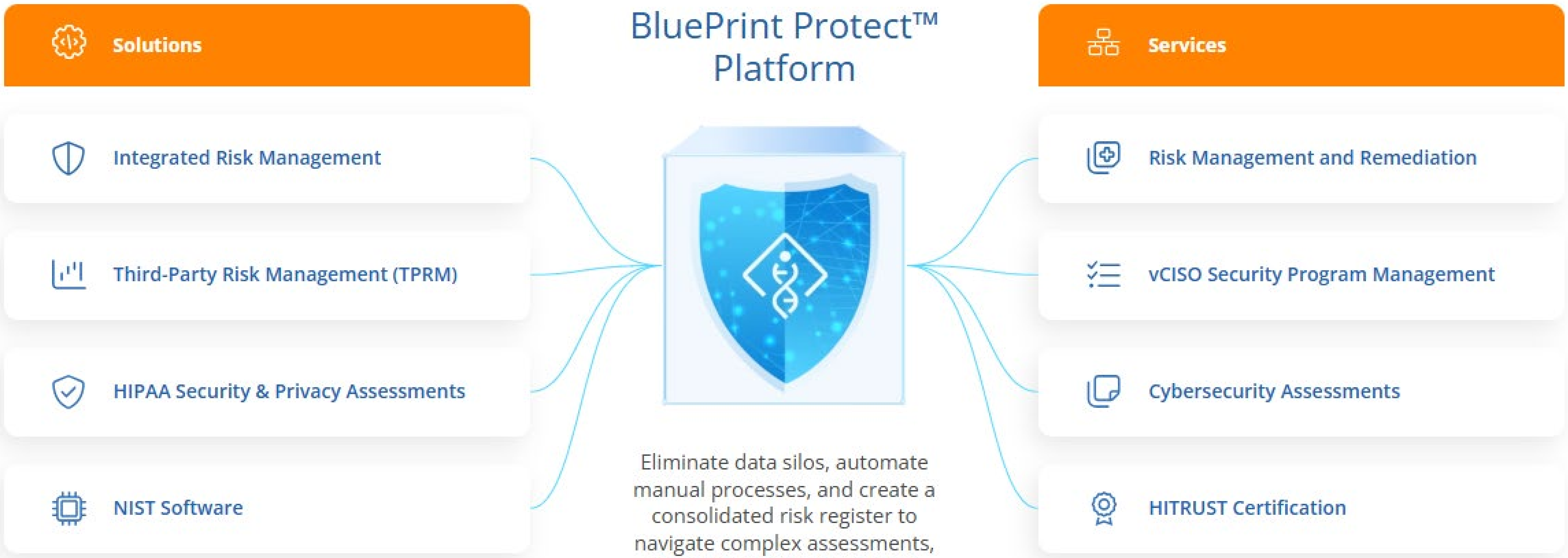
Centralize all risks layers into one view for monitoring, corrective action, and remediation.

Integrate multiple industry risk management frameworks to amplify readiness and remediation

Aggregate and normalize external insights via APIs for a consolidated risk outlook

Leverage optimization and assessor support to amplify security programs

Intraprise Health 101



BluePrint Protect™ Platform

Solutions

- Integrated Risk Management
- Third-Party Risk Management (TPRM)
- HIPAA Security & Privacy Assessments
- NIST Software

Services

- Risk Management and Remediation
- vCISO Security Program Management
- Cybersecurity Assessments
- HITRUST Certification

Eliminate data silos, automate manual processes, and create a consolidated risk register to navigate complex assessments, evaluate risk trade-offs, and maintain compliance with a single source of truth.

KLAS Research Cybersecurity Analysis

We achieved the highest KLAS score for Security and Privacy Consulting Services and Product Companies in the September 2024 Report.

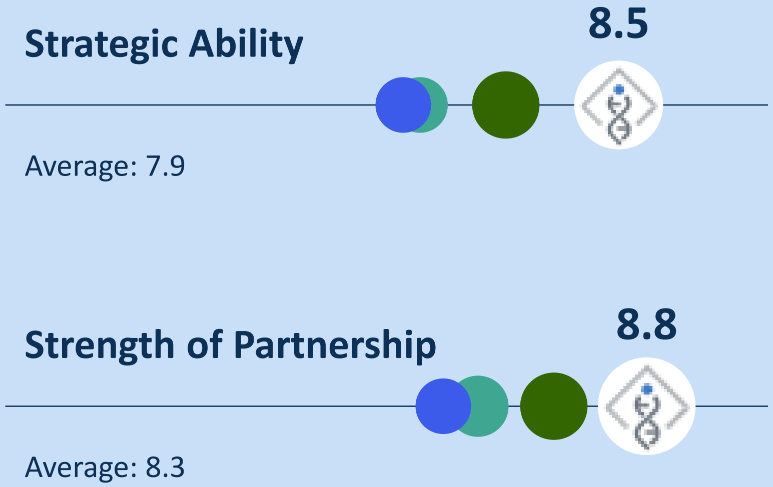
Average Score

Intraprise HEALTH	95.0
MEDITOLOGY SERVICES	92.4
Fortified HEALTH SECURITY	88.4
Clearwater	87.5

Score Breakdown

Would you buy again?	100% Yes
Likely to Recommend	8.9 / 9.0
Overall Satisfaction	8.6 / 9.0
Engagement Execution	8.4 / 9.0
Quality of Staff / Consultants	8.1 / 9.0
Strategic Ability	8.5 / 9.0
Executive Involvement	8.5 / 9.0
Strength of Partnership	8.8 / 9.0
Avoids Charging for Every Little Thing	100% Yes
Exceeds Expectations	88% Yes
Money’s Worth	8.8 / 9.0
Drives Tangible Outcomes	8.2 / 9.0

Greatest Differentiators vs. Our Competition:

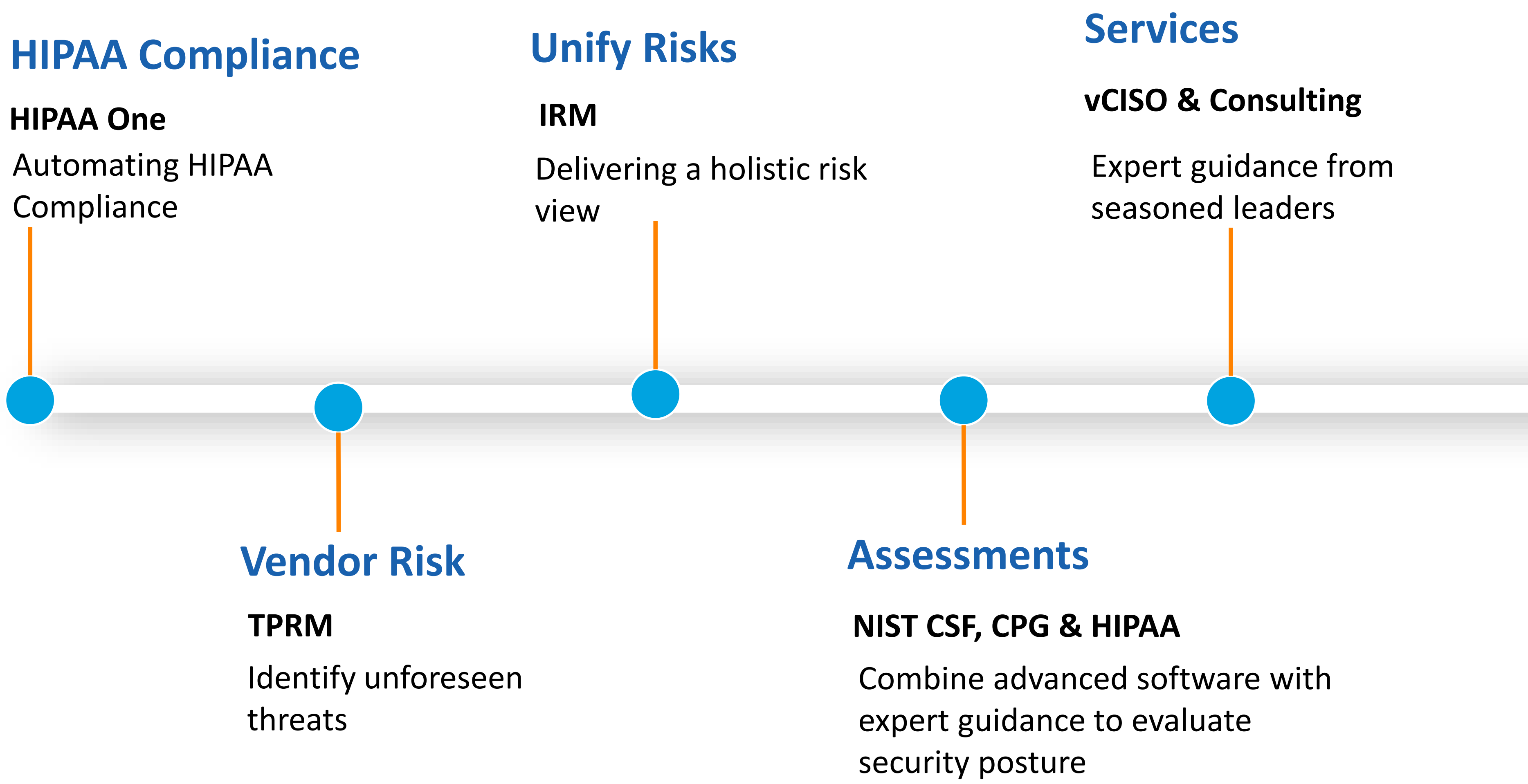


Note: Only KLAS category for cybersecurity.

Pathway to Prevention:
Adopting a Holistic Cybersecurity Program

Pathway to Prevention: Building Your Program

Meeting Clients Where They Are At



HIPAA Compliance

HIPAA One

Automating HIPAA Compliance

Vendor Risk

TPRM

Identify unforeseen threats

Unify Risks

IRM

Delivering a holistic risk view

Assessments

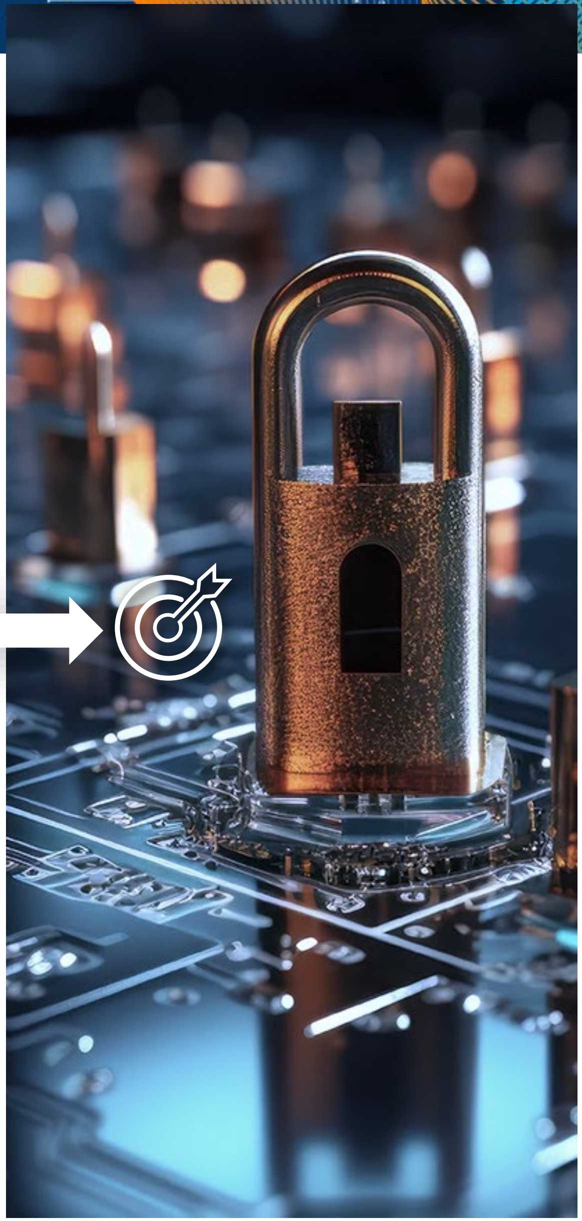
NIST CSF, CPG & HIPAA

Combine advanced software with expert guidance to evaluate security posture

Services

vCISO & Consulting

Expert guidance from seasoned leaders



Maximizing Your Investments in Other Technologies

Pathway to Prevention: Consulting Services

Program Assessment Services

Educate Board and Leadership Teams

Policy and Process Optimization

Implement Cybersecurity Best Practices with Seasoned vCISOs

Develop Tailored, Actionable Plans to Meet/Exceed CPGs

Design Governance Models and Response Protocols

Poll Question

Is your organization certified in these assessments and frameworks?

- A HITRUST
- B NIST CSF
- C HIPAA Security Risk Assessment (SRA)
- D 405(d) Health Industry Cybersecurity Practices (HICP)
- E I am not sure

Questions to Ask to Jump-Start Your TPRM Program

Secure Executive Buy-in

Leadership Engagement - Keep It Simple

Keep It High-Level

- Share insights on current state of cybersecurity

Know Your Issues

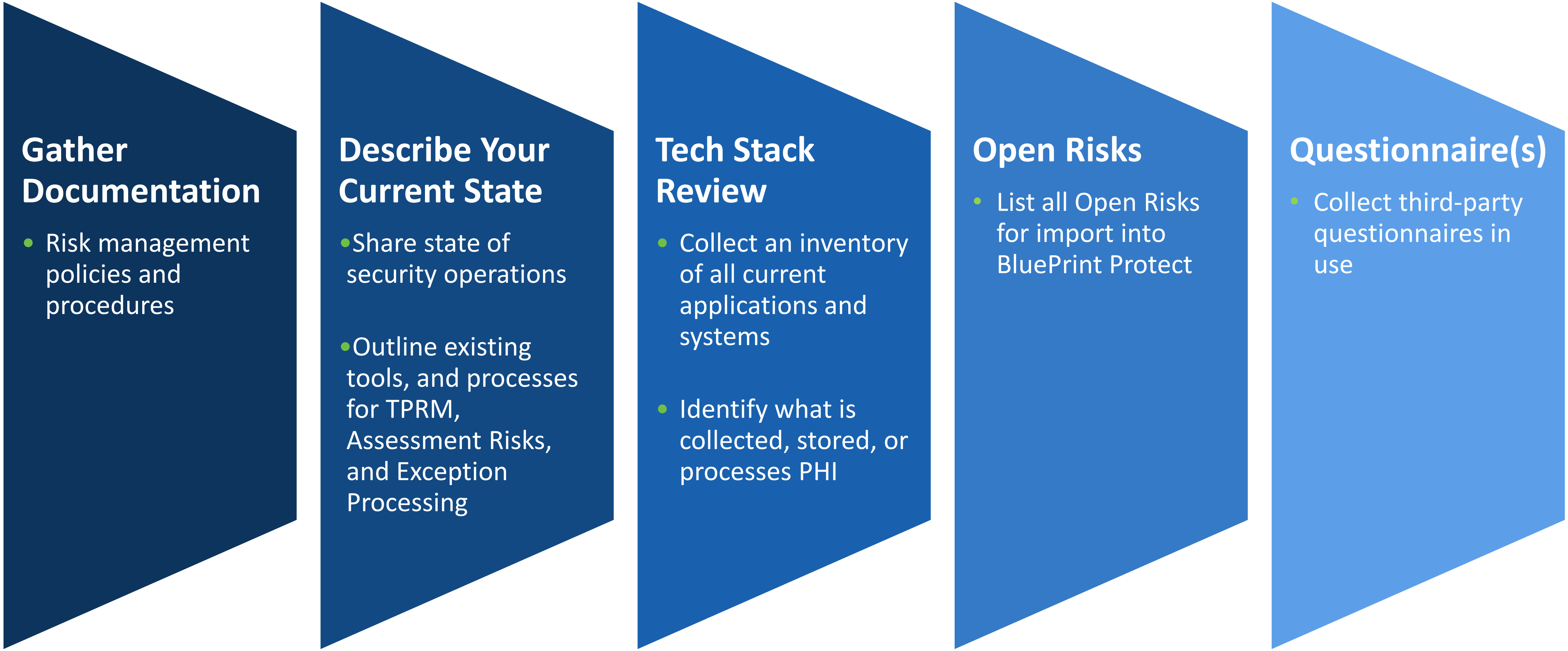
- Leaders have a vested interest
- Share operational gaps

Define Your Risk Tolerance

- Ensure alignment with cybersecurity strategy, priorities, and financial impact

Reimagining Cybersecurity

Modernizing Your Cybersecurity Program



Gather Documentation

- Risk management policies and procedures

Describe Your Current State

- Share state of security operations
- Outline existing tools, and processes for TPRM, Assessment Risks, and Exception Processing

Tech Stack Review

- Collect an inventory of all current applications and systems
- Identify what is collected, stored, or processes PHI

Open Risks

- List all Open Risks for import into BluePrint Protect

Questionnaire(s)

- Collect third-party questionnaires in use

Valley Health System's Story

Challenge

- Scaling and Managing Vendor Risk
- Managing IoT

Solution

- Deployed an Agnostic Risk Management Platform
- Aggregates Third-Party Frameworks, Assessments
- Delivers a 360-Risk View

Client: A 451- Bed Healthcare System

> We’ve streamlined our risk management initiatives, allowing us to meet operational goals and deliver high-quality, patient care with minimal project delays.

Miroslav Belote
Valley Health System

Q & A

Contact Us

Comprehensive Support

If you have any questions or would like to explore how Intraprise Health by Health Catalyst can enhance your cybersecurity program, please reach out to our team. We look forward to working with you!

Contact Information

Email

hcwebinars@healthcatalyst.com

Website

intraprisehealth.com
Healthcatalyst.com

Social Media

Intraprise Health

Health Catalyst

Thank You!