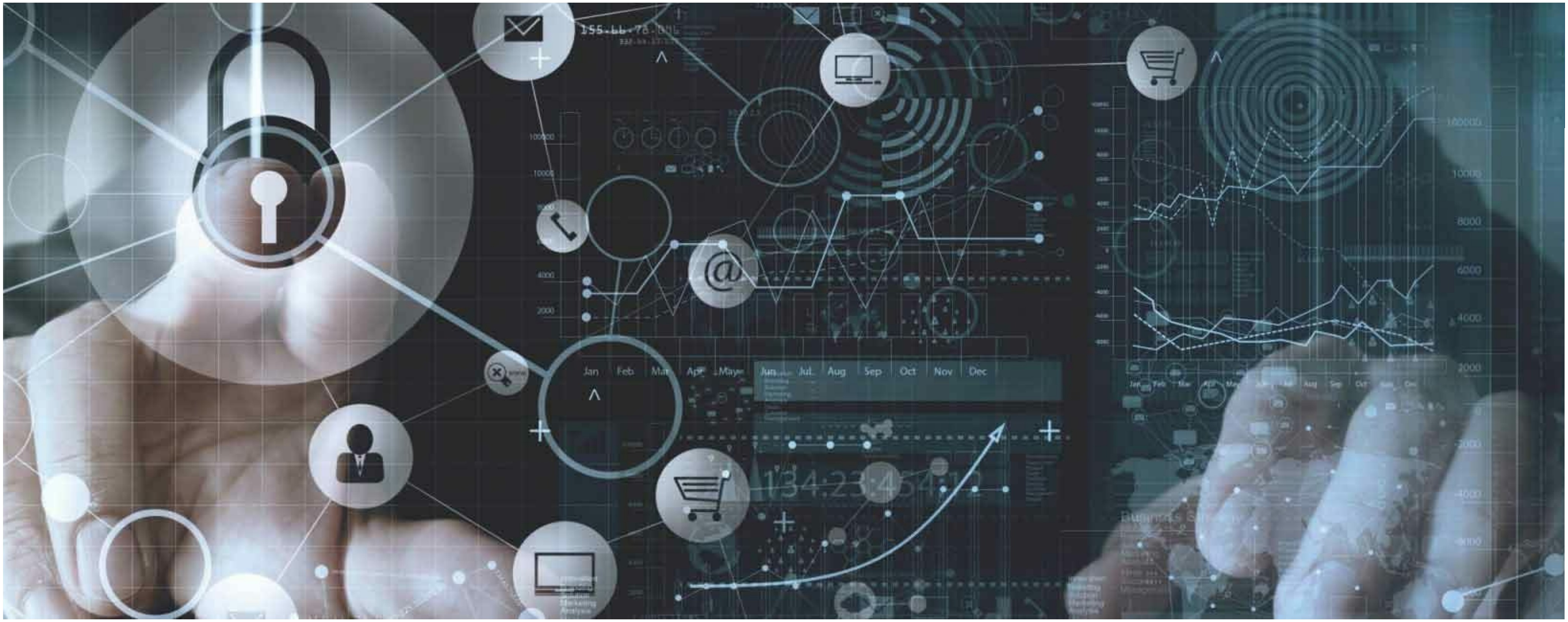


OSCAL Workshop:
Applicability of OSCAL for Healthcare

March 2nd, 2022

Intraprise HEALTH

Our Presenter

Intraprise HEALTH

Vikas Khosla
Chief Digital Health Security Officer

- 20+ years in Healthcare Security, Privacy and Compliance
- Previously founded and lead 100% healthcare security consultancy
- Focused on optimization of enterprise security programs
- Host of “Virtual Coffee Chats with Vikas” podcast

Agenda

- Current Landscape and Regulations in Healthcare
- Special Challenges in the Healthcare Sector
- The Need for Scalability and Standards
- Sample of OSCAL Automation
- OSCAL APIs: Achieving a ”Single Pane of Glass View of Risks”
- Q&A

Healthcare Sector Feeling
"Cybersecurity-Pressure"

Intraprise HEALTH

34%
Share of global healthcare sector suffering a ransomware attack in the last year
(Source: HHS)

33%
Percentage of all third-party breaches targeting healthcare
(Source: Black Kite)

$250 **value of a Healthcare Record**

$5 **value of Credit Card data**

(Source: Trustwave)

45,000,000
Number of healthcare records stolen or exposed in 2021

(Source: HIPAA Journal)

8M hours - $2B annually
Healthcare industry level of effort and cost to perform a manual HIPAA Security Assessment

*Includes physician practices, hospitals and health insurers

(Source: Intraprise Health)

Tailwinds for Adopting Cybersecurity Automation

Intraprise HEALTH

Recent Events and Legislation

Stark Safe Harbor

- Allows for the donation of cybersecurity technology (including hardware) and related services if certain conditions are met.

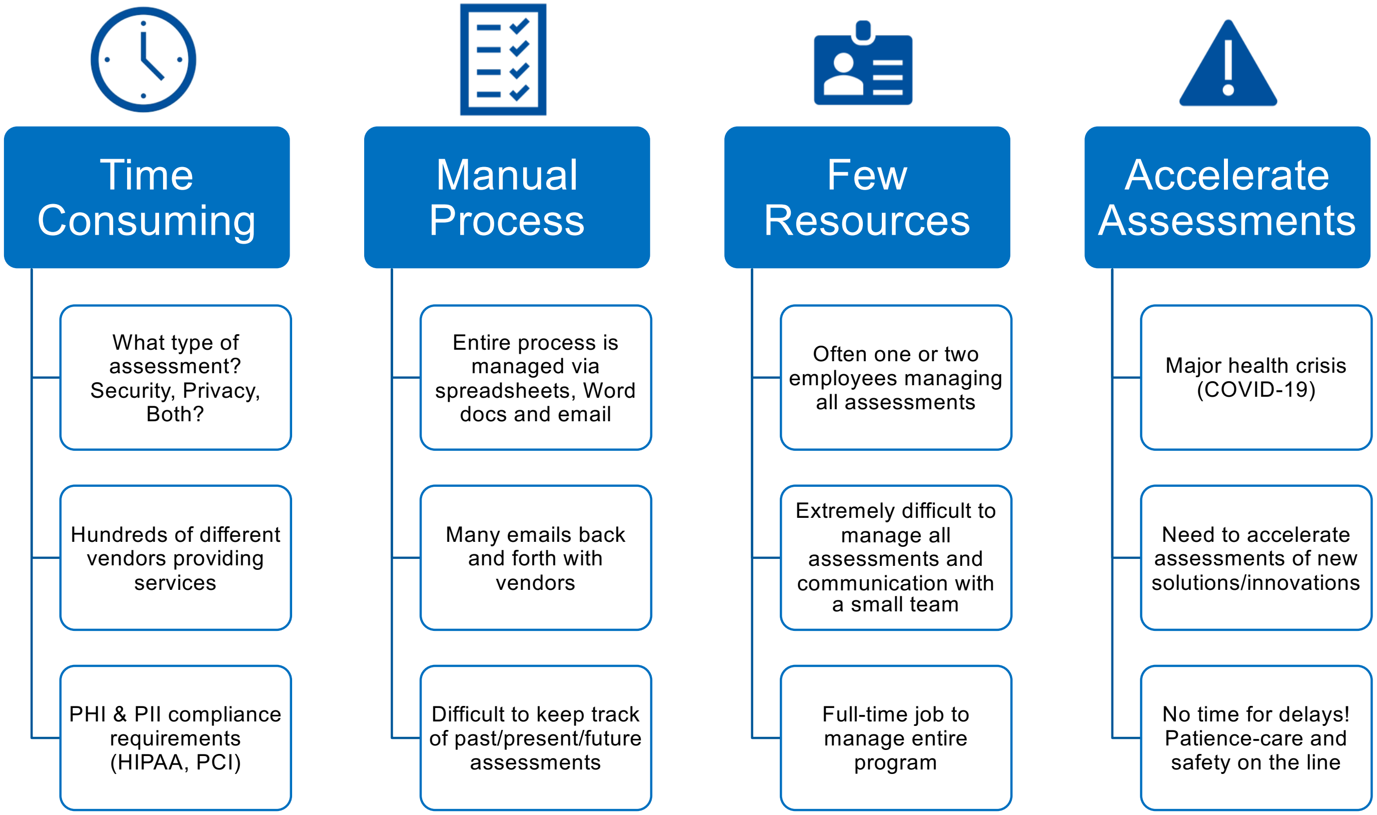
HIPAA Privacy Rule Proposed Changes

- Better support individuals' engagement in their care, remove barriers to coordinated care, and reduce regulatory burdens on the healthcare industry

HIPAA/HITECH Safe Harbor (H.R. 7898)

- When investigating/undertaking HIPAA enforcement the legislation directs HHS to consider the use of industry-standard security practices, cybersecurity preparedness when calculating fines, and decreased audit lengths.

Industry-wide Challenges



Time Consuming

- What type of assessment? Security, Privacy, Both?
- Hundreds of different vendors providing services
- PHI & PII compliance requirements (HIPAA, PCI)

Manual Process

- Entire process is managed via spreadsheets, Word docs and email
- Many emails back and forth with vendors
- Difficult to keep track of past/present/future assessments

Few Resources

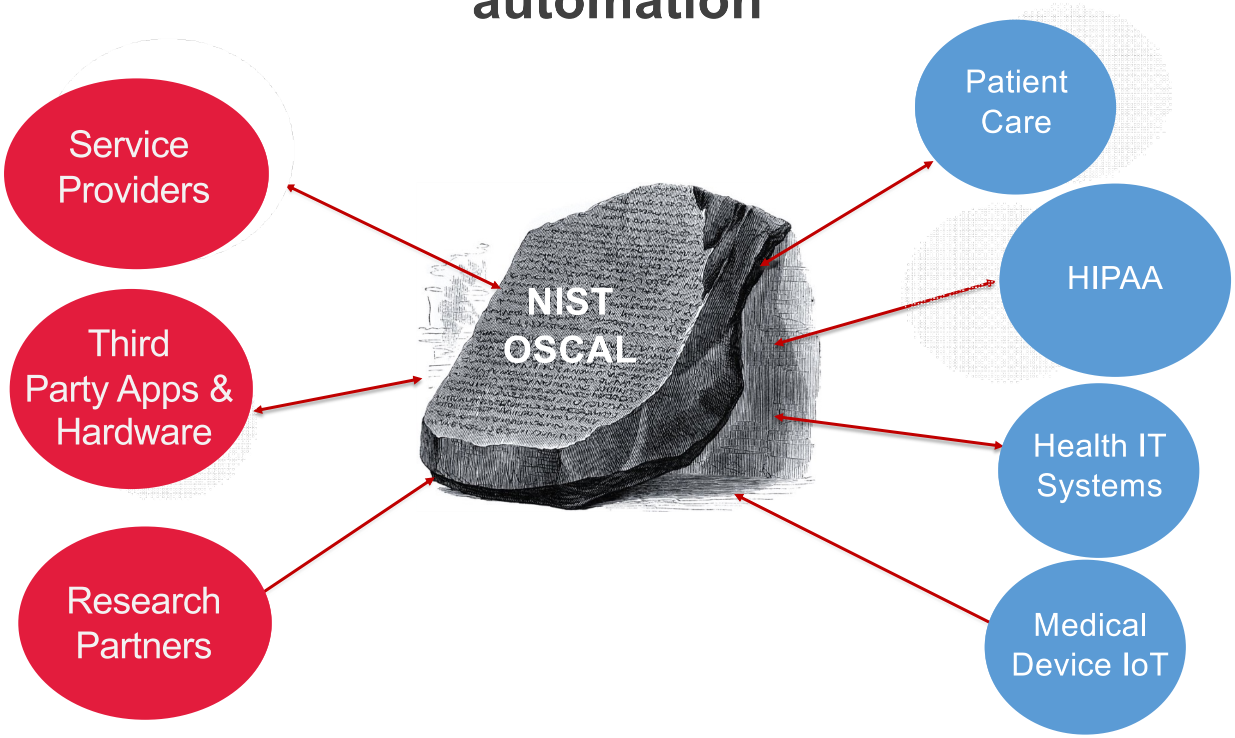
- Often one or two employees managing all assessments
- Extremely difficult to manage all assessments and communication with a small team
- Full-time job to manage entire program

Accelerate Assessments

- Major health crisis (COVID-19)
- Need to accelerate assessments of new solutions/innovations
- No time for delays! Patience-care and safety on the line

“The Rosetta Stone” for Healthcare Assessors

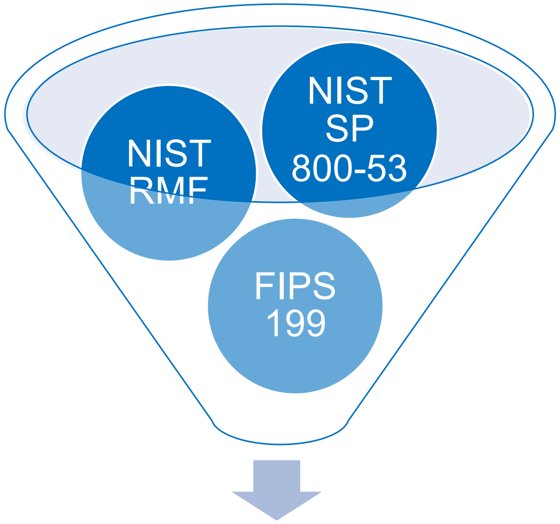
OSCAL enables tools and organizations to exchange risk information via automation



OSCAL sets the foundation for automation and interoperability

An Efficient Compliance and Security Program using OSCAL

Intraprise HEALTH

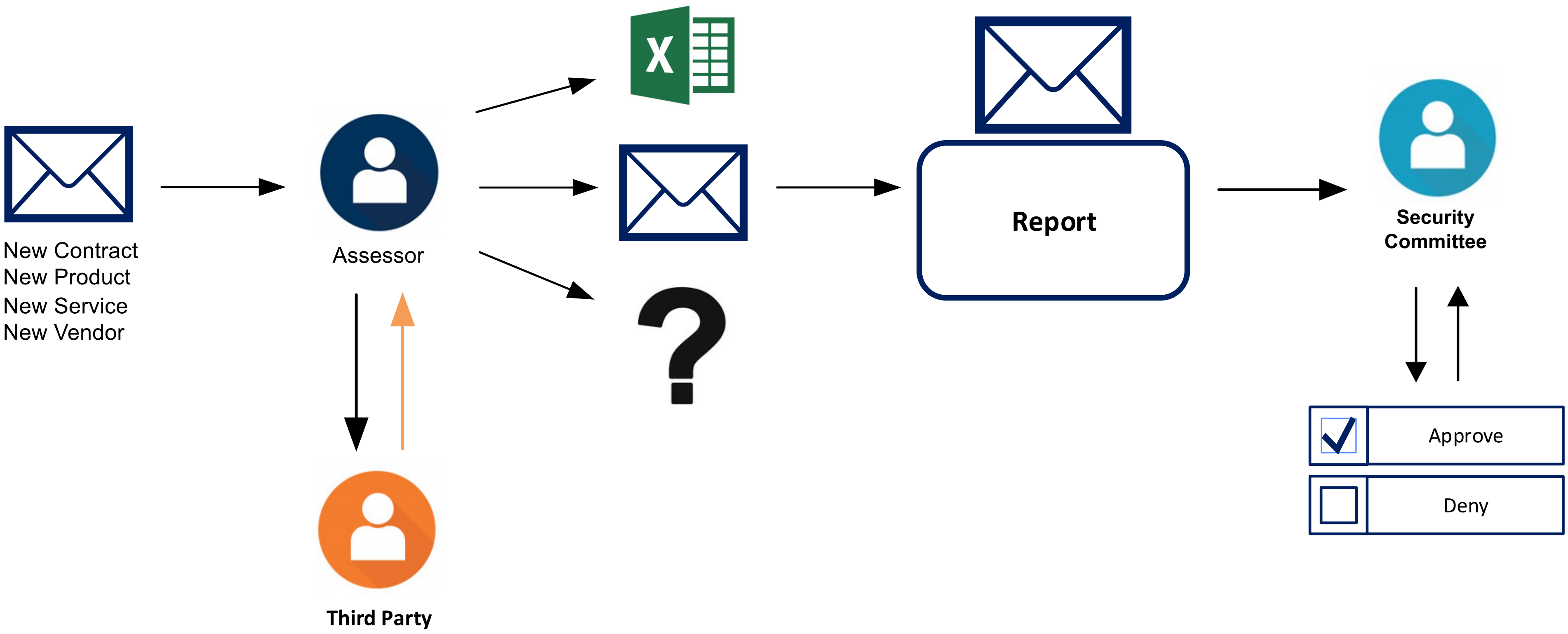


HIPAA, HITECH, FISMA

Building a Centralized Repository of Compliance Standards and Risk Data using OSCAL

- Utilize Standards to accelerate Compliance and Cyber-Resilience
- *"Single-Pane of Glass" View of Risks –* Unified, Normalized and Interoperable
- Scalable across healthcare sector participants
- Significant overlap of companies doing business with federal and healthcare sector customers

Before: Manual Third-Party Assessment Process



New Contract
New Product
New Service
New Vendor

Assessor

Third Party

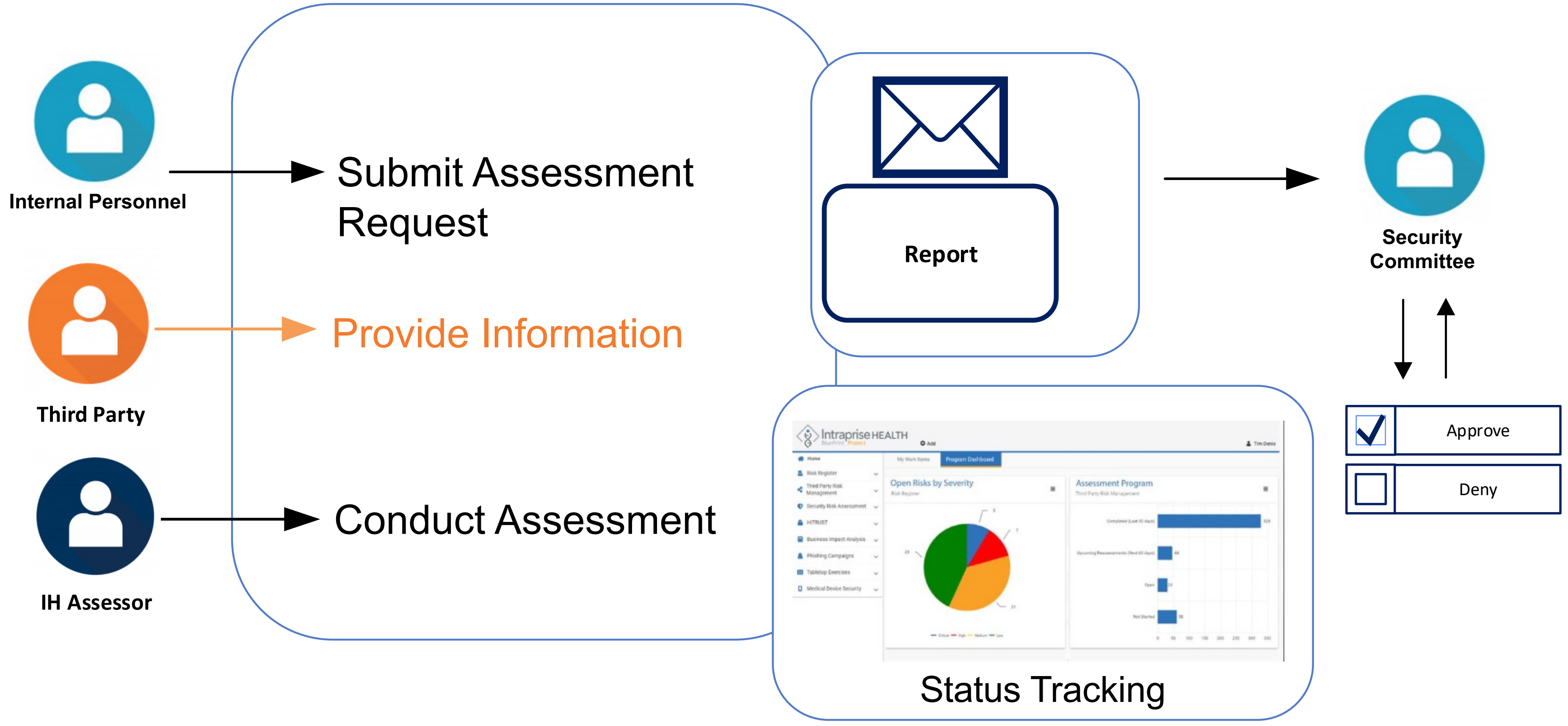
Report

Security Committee

☑ Approve

□ Deny

After: Automated Third-Party Assessment Process



Internal Personnel

Submit Assessment Request

Third Party

Provide Information

IH Assessor

Conduct Assessment

Report

Security Committee

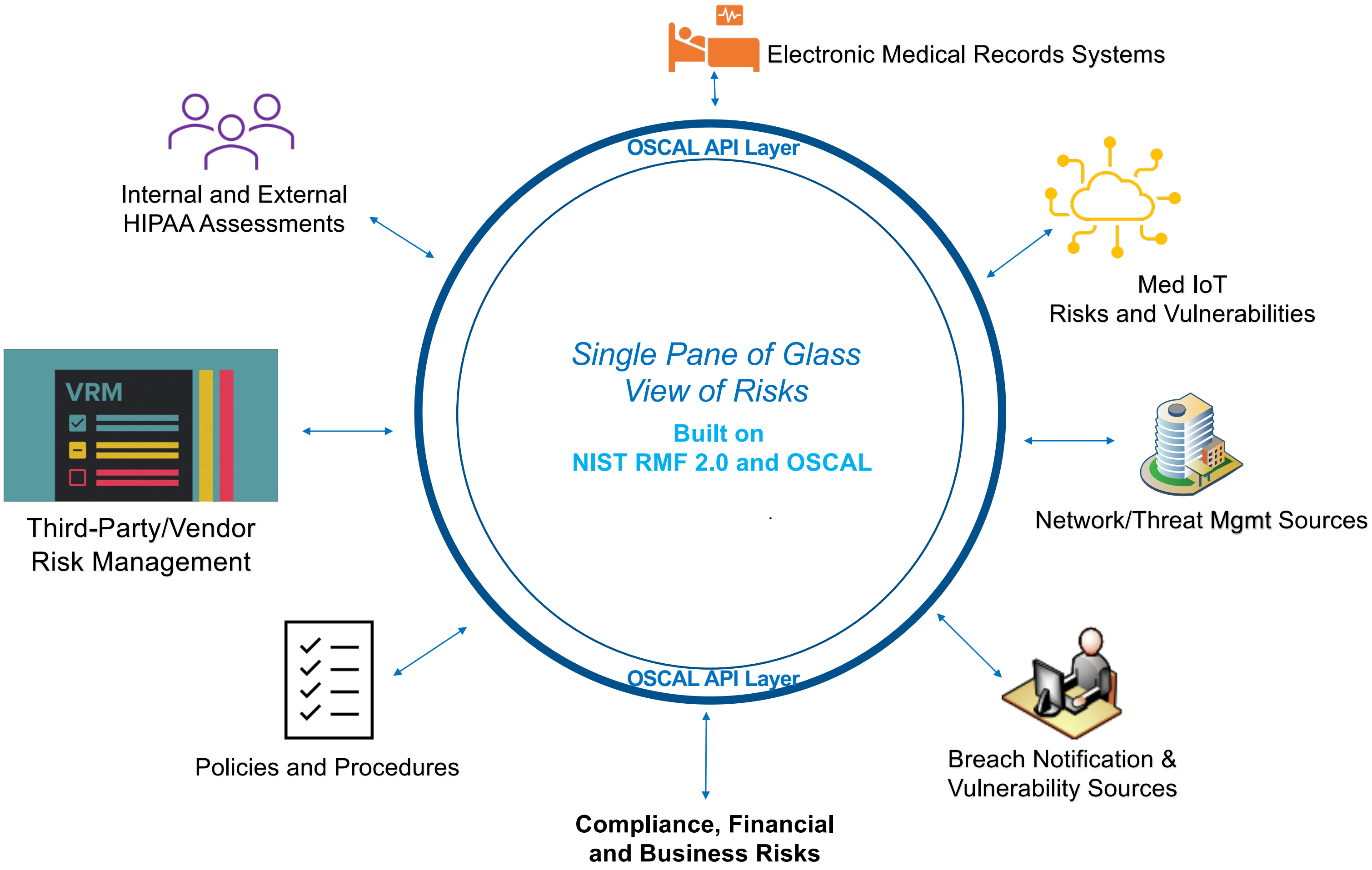
☑ Approve

□ Deny

Status Tracking

OSCAL and RMF enabled
Integrated Risk Management

Intraprise HEALTH



Electronic Medical Records Systems

Internal and External HIPAA Assessments

Med IoT Risks and Vulnerabilities

OSCAL API Layer

Single Pane of Glass View of Risks

Built on NIST RMF 2.0 and OSCAL

OSCAL API Layer

Third-Party/Vendor Risk Management

Network/Threat Mgmt Sources

Policies and Procedures

Breach Notification & Vulnerability Sources

Compliance, Financial and Business Risks

HIPAA and NIST Security and Privacy Risk Assessments

TPRM Assessments

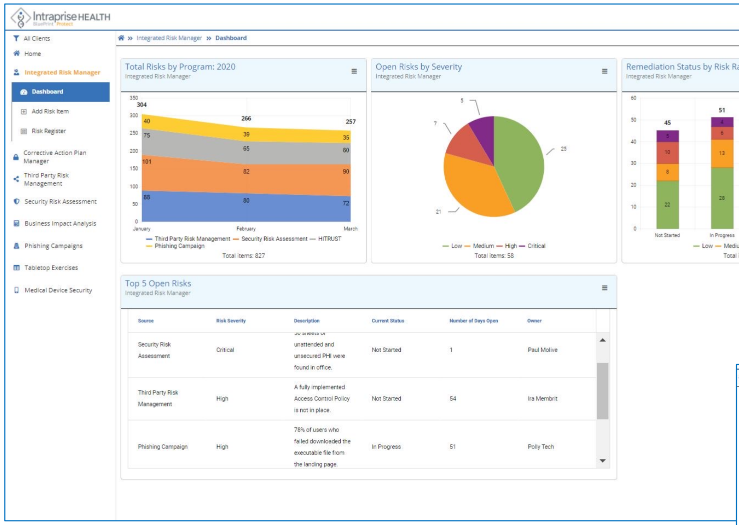
Portfolio Manager

Plan-of-Action Manager

Enterprise Risk Register, Dashboards and Analytics

Informed Decision Making

- Enterprise, Holistic View
- Drive Program Maturity
- Assessment and Workflow Automation
- Analytics and Visualizations

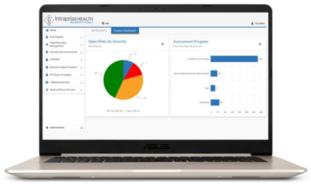


Top 5 Open Risks

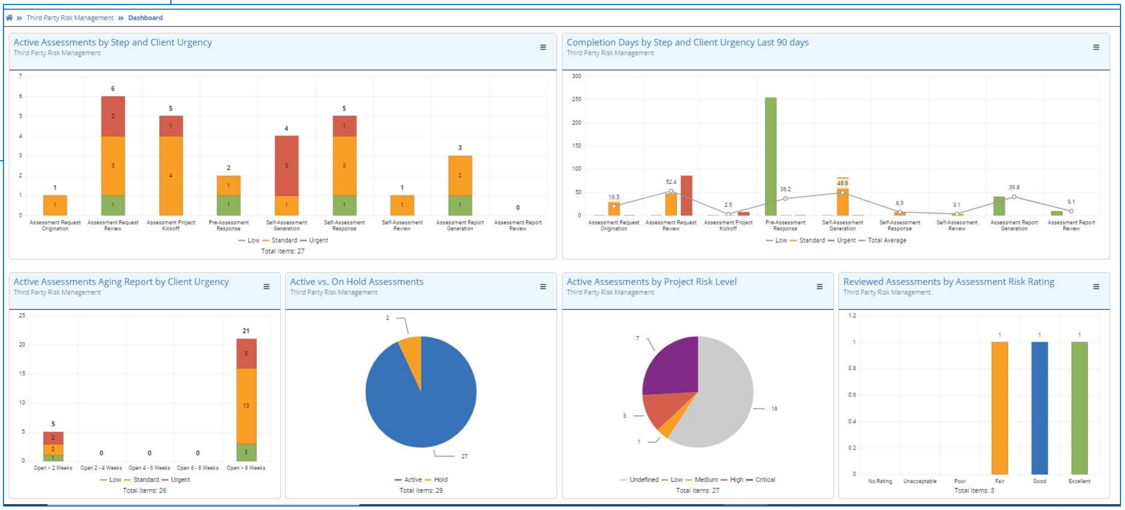
Integrated Risk Manager

Source	Risk Severity	Description	Current Status	Number of Days Open	Owner
Security Risk Assessment	Critical	50 sheets of unattended and unsecured PHI were found in office.	Not Started	1	Paul Molive
Third Party Risk Management	High	A fully implemented Access Control Policy is not in place.	Not Started	54	Ira Membrit
Phishing Campaign	High	78% of users who failed downloaded the executable file from the landing page.	In Progress	51	Polly Tech

IRM Dashboards



TPRM Dashboards



Third Party Risk Management » Dashboard
Active Assessments by Step and Client Urgency
Third Party Risk Management
7
6
5
4
3
2
1
0
1
1
6
2
3
1
5
1
4
2
1
1
4
3
1
5
1
3
1
1
1
3
2
1
0
Assessment Request Origination
Assessment Request Review
Assessment Project Kickoff
Pre-Assessment Response
Self-Assessment Generation
Self-Assessment Response
Self-Assessment Review
Assessment Report Generation
Assessment Report Review
Low
Standard
Urgent
Total items: 27
Completion Days by Step and Client Urgency Last 90 days
Third Party Risk Management
300
250
200
150
100
50
0
19.5
52.4
2.5
36.2
48.8
6.9
3.1
39.8
9.1
Assessment Request Origination
Assessment Request Review
Assessment Project Kickoff
Pre-Assessment Response
Self-Assessment Generation
Self-Assessment Response
Self-Assessment Review
Assessment Report Generation
Assessment Report Review
Low
Standard
Urgent
Total Average
Active Assessments Aging Report by Client Urgency
Third Party Risk Management
25
20
15
10
5
0
5
2
2
1
0
0
0
21
5
13
3
Open < 2 Weeks
Open 2 - 4 Weeks
Open 4 - 6 Weeks
Open 6 - 8 Weeks
Open > 8 Weeks
Low
Standard
Urgent
Total items: 26
Active vs. On Hold Assessments
Third Party Risk Management
2
27
Active
Hold
Total items: 29
Active Assessments by Project Risk Level
Third Party Risk Management
7
3
1
16
Undefined
Low
Medium
High
Critical
Total items: 27
Reviewed Assessments by Assessment Risk Rating
Third Party Risk Management
1.2
1
0.8
0.6
0.4
0.2
0
1
1
1
No Rating
Unacceptable
Poor
Fair
Good
Excellent
Total items: 3