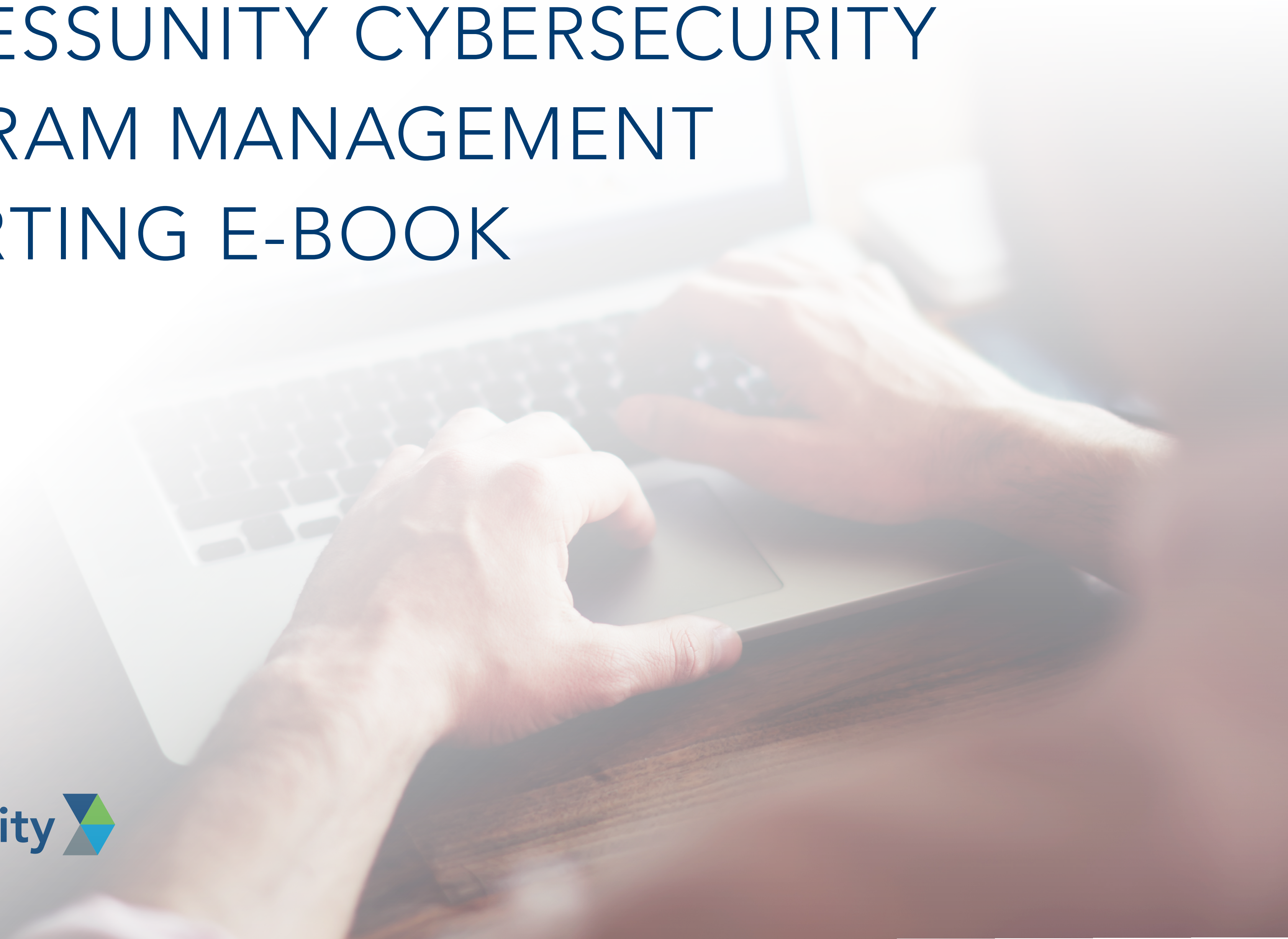
PROCESSUNITY CYBERSECURITY PROGRAM MANAGEMENT REPORTING E-BOOK



ProcessUnity

Reporting is a critical aspect of successful Cybersecurity Program Management. Whether it's accessing the best reports to give you instant insight into threats, risks or activities that require your attention or to help you prepare for an upcoming board meeting, reports and dashboards are important to fully understand the current state of your cybersecurity program. You need a consistent way to answer critical questions including:

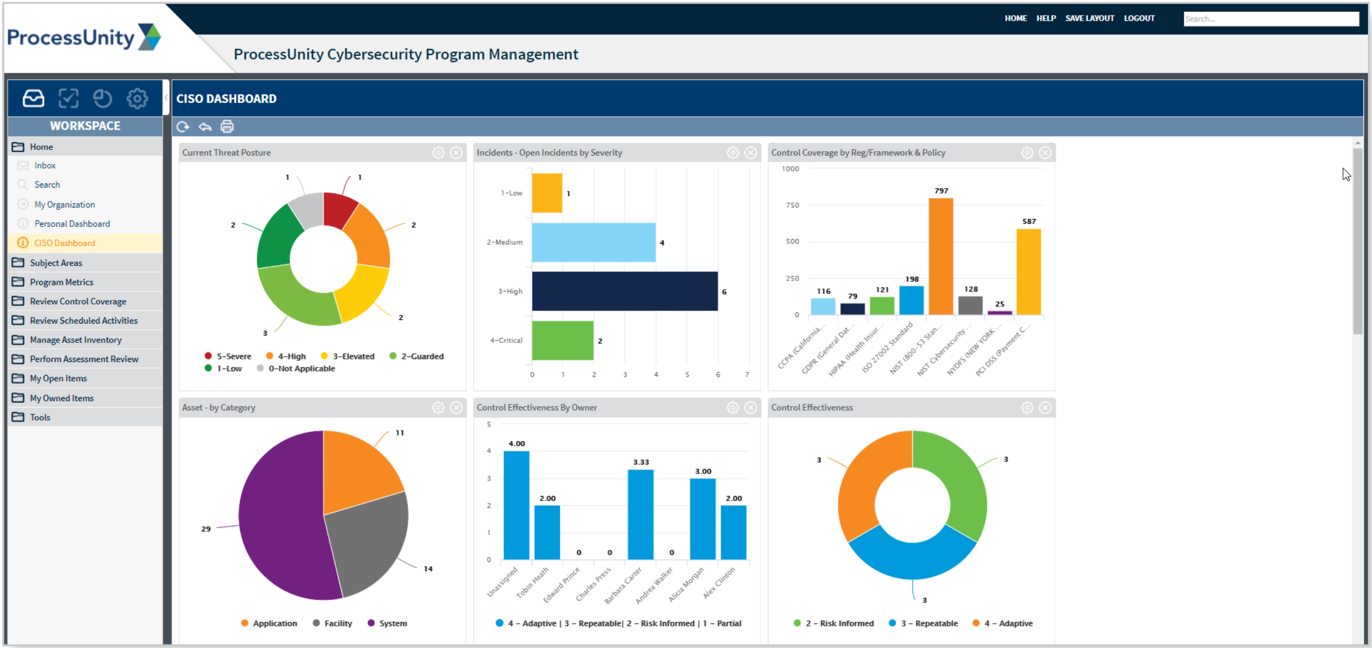
- Where are your greatest risks?
- How will you fix them?
- How much will that cost?

While ProcessUnity's simple-to-use interface allows your team to easily build custom views and display them in a personalized dashboard, ProcessUnity Cybersecurity Program Management also contains a built-in, extensive reports library to deliver at-a-glance details on the current level of threats, risks, policies, controls, issues and incidents enterprise-wide. These reports can provide you with insights into areas of concern, help you to prioritize investments and accelerate remediation.

This booklet contains a sample of the most critical reports and dashboards that CISOs and their teams need to run an effective and efficient cybersecurity management program.

> Next *CISO Dashboard*

CISO DASHBOARD



What is it?

The CISO Dashboard provides an overview of your organization's current threat posture, open incidents, control coverage, high-value assets by category and control effectiveness.

Why do you need it?

This customizable view of key activities across the program enables the CISO to quickly understand the state of their cybersecurity program. These reports readily display details in areas of concern, lend insight to accelerate remediation and help the CISO prioritize where future investment should be made.

> Next *Compliance Dashboard*

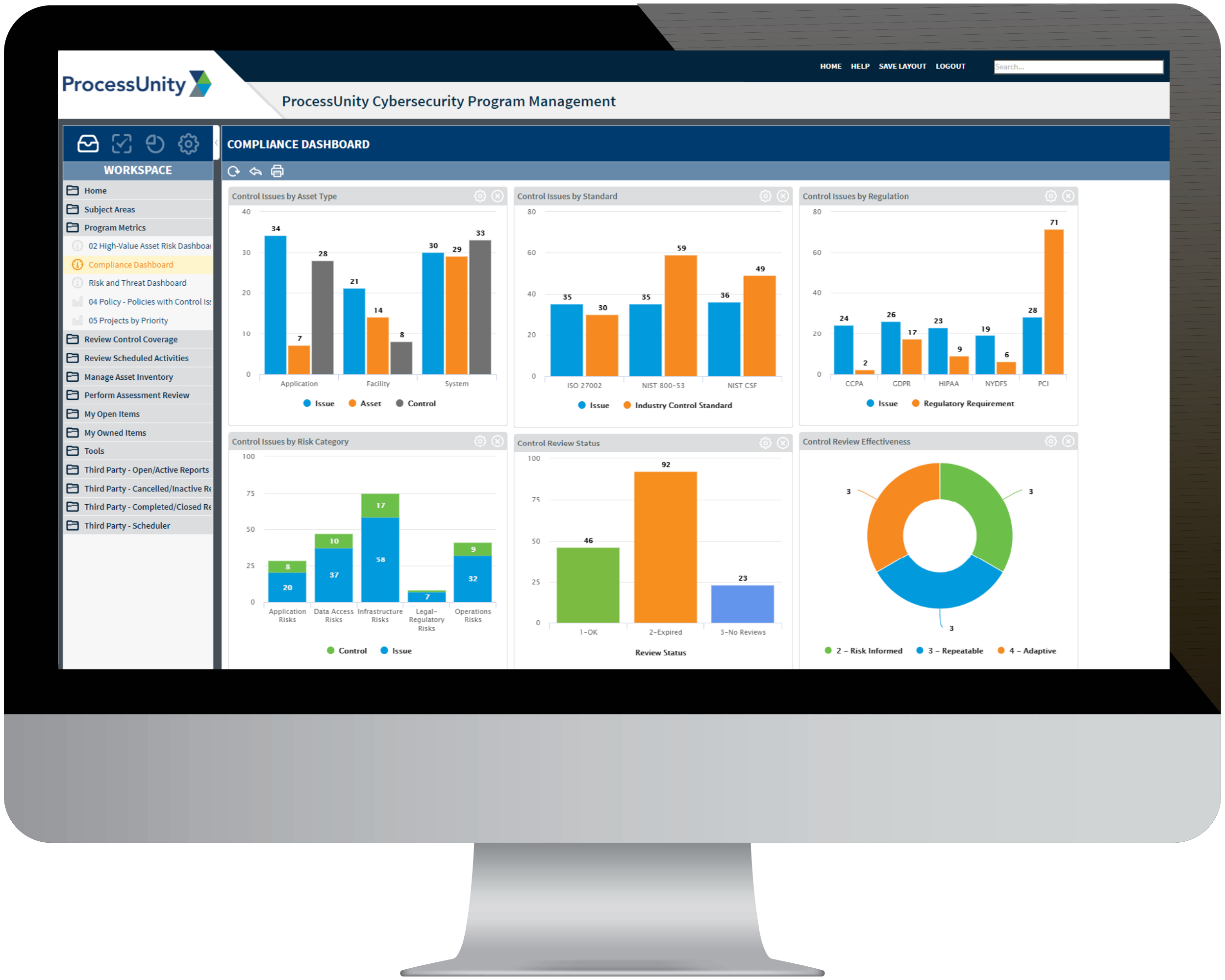
COMPLIANCE DASHBOARD

What is it?

The Compliance Dashboard details control issues by asset type, standards, regulations and risk category as well as your overall control review status and control effectiveness.

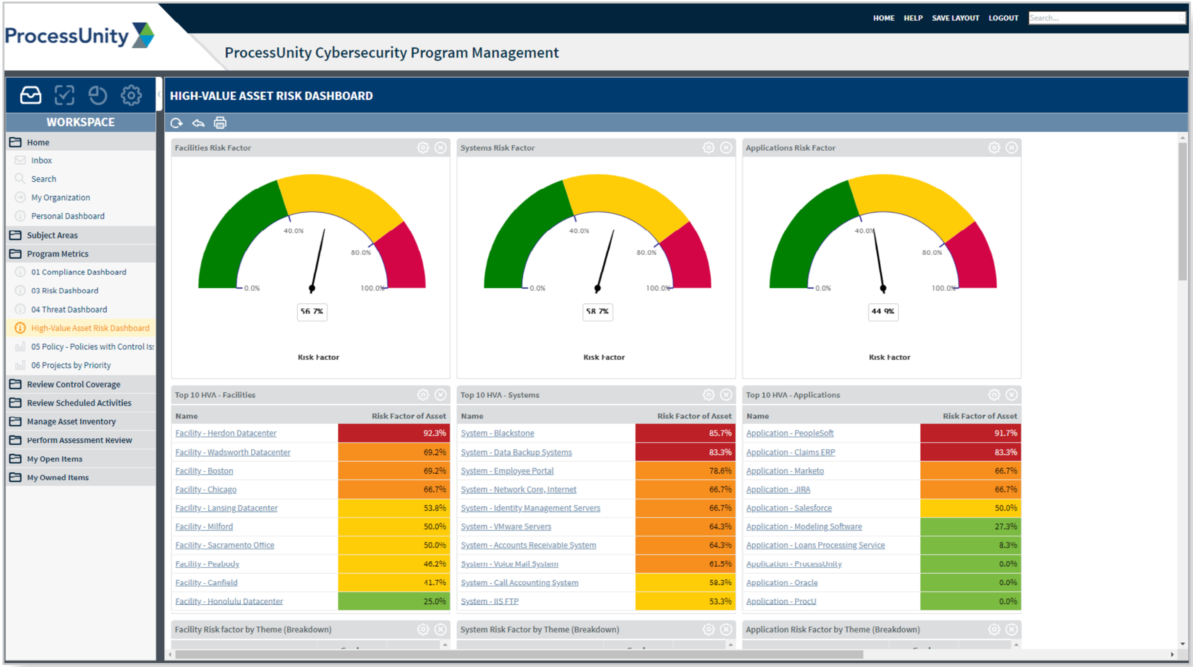
Why do you need it?

This dashboard contains critical information on the up-to-date status of control issues and control reviews. By seeing your issues broken down by asset type, standard and regulation, you know where to spend your time or make improvements to your controls. Drilling down into these reports allows for a greater understanding of when reviews were performed on each control standard, who owns each, the control's effectiveness and other information critical to maintaining cybersecurity compliance.



> Next *High-Value Asset Dashboard*

HIGH-VALUE ASSET DASHBOARD



Top 10 HVA - Facilities

Name	Risk Factor of Asset
Facility - Herdon Datacenter	92.3%
Facility - Wadsworth Datacenter	69.2%
Facility - Boston	69.2%
Facility - Chicago	66.7%
Facility - Lansing Datacenter	53.8%
Facility - Milford	50.0%
Facility - Sacramento Office	50.0%
Facility - Peabody	46.2%
Facility - Canfield	41.7%
Facility - Honolulu Datacenter	25.0%

Top 10 HVA - Systems

Name	Risk Factor of Asset
System - Blackstone	85.7%
System - Data Backup Systems	83.3%
System - Employee Portal	78.6%
System - Network Core, Internet	66.7%
System - Identity Management Servers	66.7%
System - VMware Servers	64.3%
System - Accounts Receivable System	64.3%
System - Voice Mail System	61.5%
System - Call Accounting System	58.3%
System - IIS FTP	53.3%

Top 10 HVA - Applications

Name	Risk Factor of Asset
Application - PeopleSoft	91.7%
Application - Claims ERP	83.3%
Application - Marketo	66.7%
Application - JIRA	66.7%
Application - Salesforce	50.0%
Application - Modeling Software	27.3%
Application - Loans Processing Service	8.3%
Application - ProcessUnity	0.0%
Application - Oracle	0.0%
Application - ProcU	0.0%

What is it?

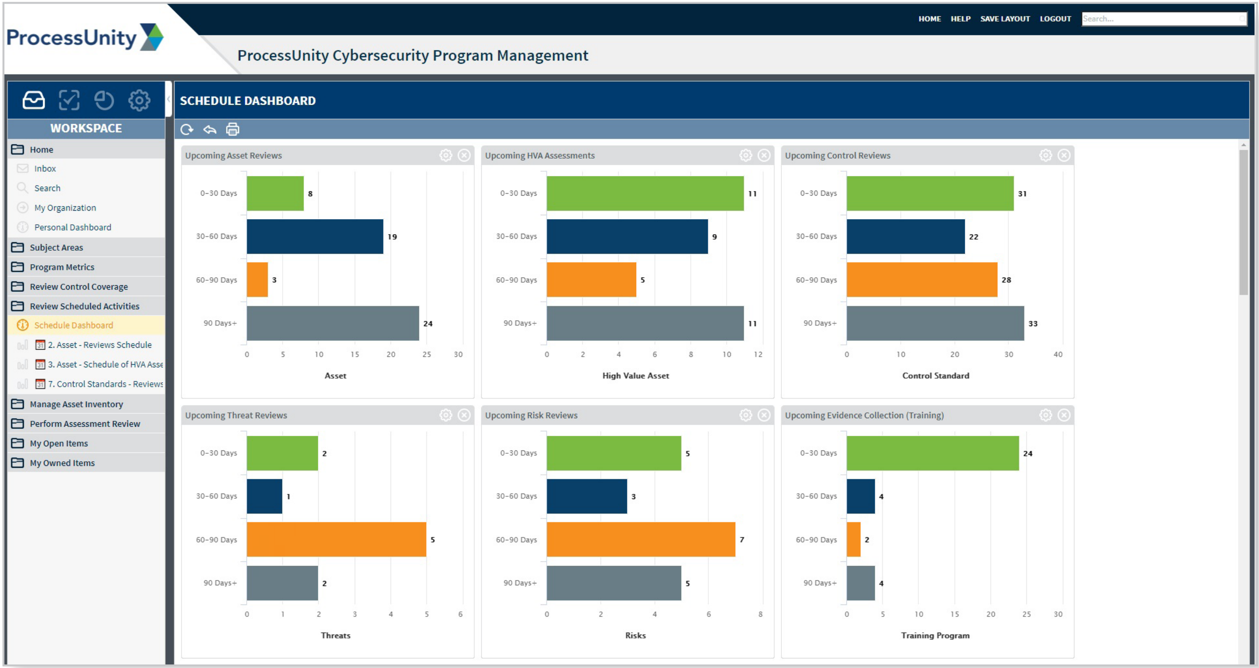
The High-Value Asset Dashboard provides an overview of the risk factor of your high-value assets such as systems, facilities and applications. Some reports display the top ten assets in each category based on their risk factor, while others aggregate the specific risk areas that impact these assets based on assessment results.

Why do you need it?

You need to monitor the status of your high-value assets across your facilities, systems and applications to understand the current state of risk. Beyond understanding the risk factor of each individual asset, this dashboard can help you identify themes across asset categories and lends insight into which controls need to be examined.

> Next *Schedule Dashboard*

SCHEDULE DASHBOARD



What is it?

This Schedule Dashboard maps out all upcoming cybersecurity related asset reviews, HVA assessments, control reviews, risk reviews and evidence collection related to training programs that are planned for the next 30, 60, 90 days and beyond.

Why do you need it?

A key component of a successful cybersecurity program is to execute all review related activities and track issues and projects to completion. The Schedule Dashboard displays all planned review and assessment activities related to your cybersecurity risk program in one screen for better planning and resource allocation. Used in conjunction with the Projects by Priority Dashboard, you can easily determine based on your team's upcoming demands which projects are next and when is the best time to tackle them based on resources.

> Next *Projects by Priority Report*

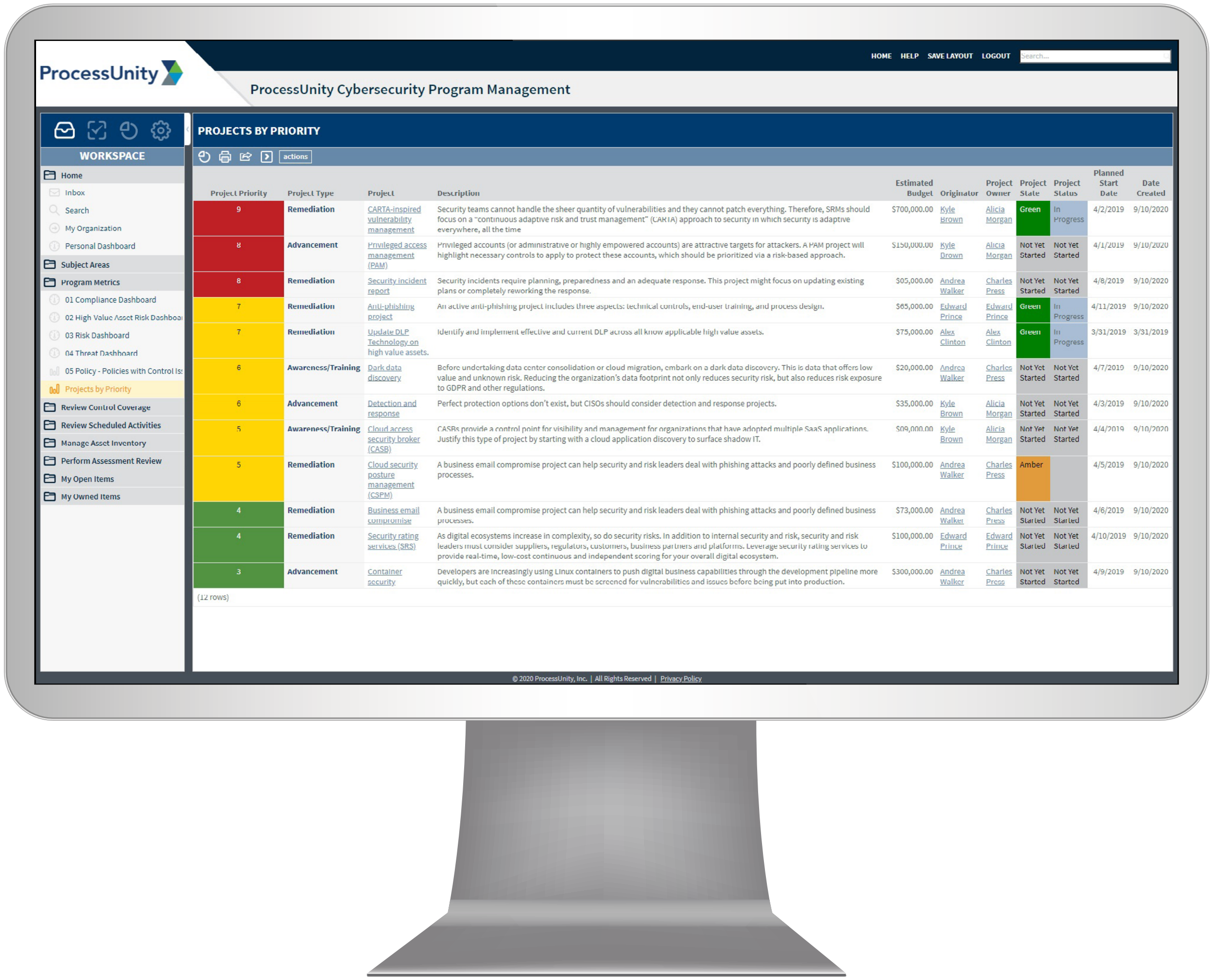
PROJECTS BY PRIORITY REPORT

What is it?

The Projects by Priority Report displays all planned – in progress and future state – projects in a priority order noting the project type, description, cost, key dates, status and those individuals responsible for originating and executing the project.

Why do you need it?

When requesting budget or reporting on status, it is critical to have a holistic and detailed, real-time view of project activity and demand across your cybersecurity program. While the CISO may not know the details of every request off the top of the head, this report can be easily exported for a quick snapshot to take to meetings and aid in budget or resource allocation discussions. This report can also be sorted into various categories to help determine what projects can be completed by what resources or within a specific timeframe.



ProcessUnity Cybersecurity Program Management

PROJECTS BY PRIORITY

Project Priority	Project Type	Project	Description	Estimated Budget	Originator	Project Owner	Project State	Project Status	Planned Start Date	Date Created
9	Remediation	CARTA-inspired vulnerability management	Security teams cannot handle the sheer quantity of vulnerabilities and they cannot patch everything. Therefore, SRMs should focus on a "continuous adaptive risk and trust management" (CARTA) approach to security in which security is adaptive everywhere, all the time	$700,000.00	Kyle Brown	Alicia Morgan	Green	In Progress	4/2/2019	9/10/2020
8	Advancement	Privileged access management (PAM)	Privileged accounts (or administrative or highly empowered accounts) are attractive targets for attackers. A PAM project will highlight necessary controls to apply to protect these accounts, which should be prioritized via a risk-based approach.	$150,000.00	Kyle Brown	Alicia Morgan	Not Yet Started	Not Yet Started	4/1/2019	9/10/2020
8	Remediation	Security incident report	Security incidents require planning, preparedness and an adequate response. This project might focus on updating existing plans or completely reworking the response.	$05,000.00	Andrea Walker	Charles Press	Not Yet Started	Not Yet Started	4/8/2019	9/10/2020
7	Remediation	Anti-phishing project	An active anti-phishing project includes three aspects: technical controls, end-user training, and process design.	$65,000.00	Edward Prince	Edward Prince	Green	In Progress	4/11/2019	9/10/2020
7	Remediation	Update DLP Technology on high value assets.	Identify and implement effective and current DLP across all know applicable high value assets.	$75,000.00	Alex Clinton	Alex Clinton	Green	In Progress	3/31/2019	3/31/2019
6	Awareness/Training	Dark data discovery	Before undertaking data center consolidation or cloud migration, embark on a dark data discovery. This is data that offers low value and unknown risk. Reducing the organization's data footprint not only reduces security risk, but also reduces risk exposure to GDPR and other regulations.	$20,000.00	Andrea Walker	Charles Press	Not Yet Started	Not Yet Started	4/7/2019	9/10/2020
6	Advancement	Detection and response	Perfect protection options don't exist, but CISOs should consider detection and response projects.	$35,000.00	Kyle Brown	Alicia Morgan	Not Yet Started	Not Yet Started	4/3/2019	9/10/2020
5	Awareness/Training	Cloud access security broker (CASB)	CASBs provide a control point for visibility and management for organizations that have adopted multiple SaaS applications. Justify this type of project by starting with a cloud application discovery to surface shadow IT.	$09,000.00	Kyle Brown	Alicia Morgan	Not Yet Started	Not Yet Started	4/4/2019	9/10/2020
5	Remediation	Cloud security posture management (CSPM)	A business email compromise project can help security and risk leaders deal with phishing attacks and poorly defined business processes.	$100,000.00	Andrea Walker	Charles Press	Amber		4/5/2019	9/10/2020
4	Remediation	Business email compromise	A business email compromise project can help security and risk leaders deal with phishing attacks and poorly defined business processes.	$73,000.00	Andrea Walker	Charles Press	Not Yet Started	Not Yet Started	4/6/2019	9/10/2020
4	Remediation	Security rating services (SRS)	As digital ecosystems increase in complexity, so do security risks. In addition to internal security and risk, security and risk leaders must consider suppliers, regulators, customers, business partners and platforms. Leverage security rating services to provide real-time, low-cost continuous and independent scoring for your overall digital ecosystem.	$100,000.00	Edward Prince	Edward Prince	Not Yet Started	Not Yet Started	4/10/2019	9/10/2020
3	Advancement	Container security	Developers are increasingly using Linux containers to push digital business capabilities through the development pipeline more quickly, but each of these containers must be screened for vulnerabilities and issues before being put into production.	$300,000.00	Andrea Walker	Charles Press	Not Yet Started	Not Yet Started	4/9/2019	9/10/2020

(12 rows)

> Next *Asset Assessments for Review Report*

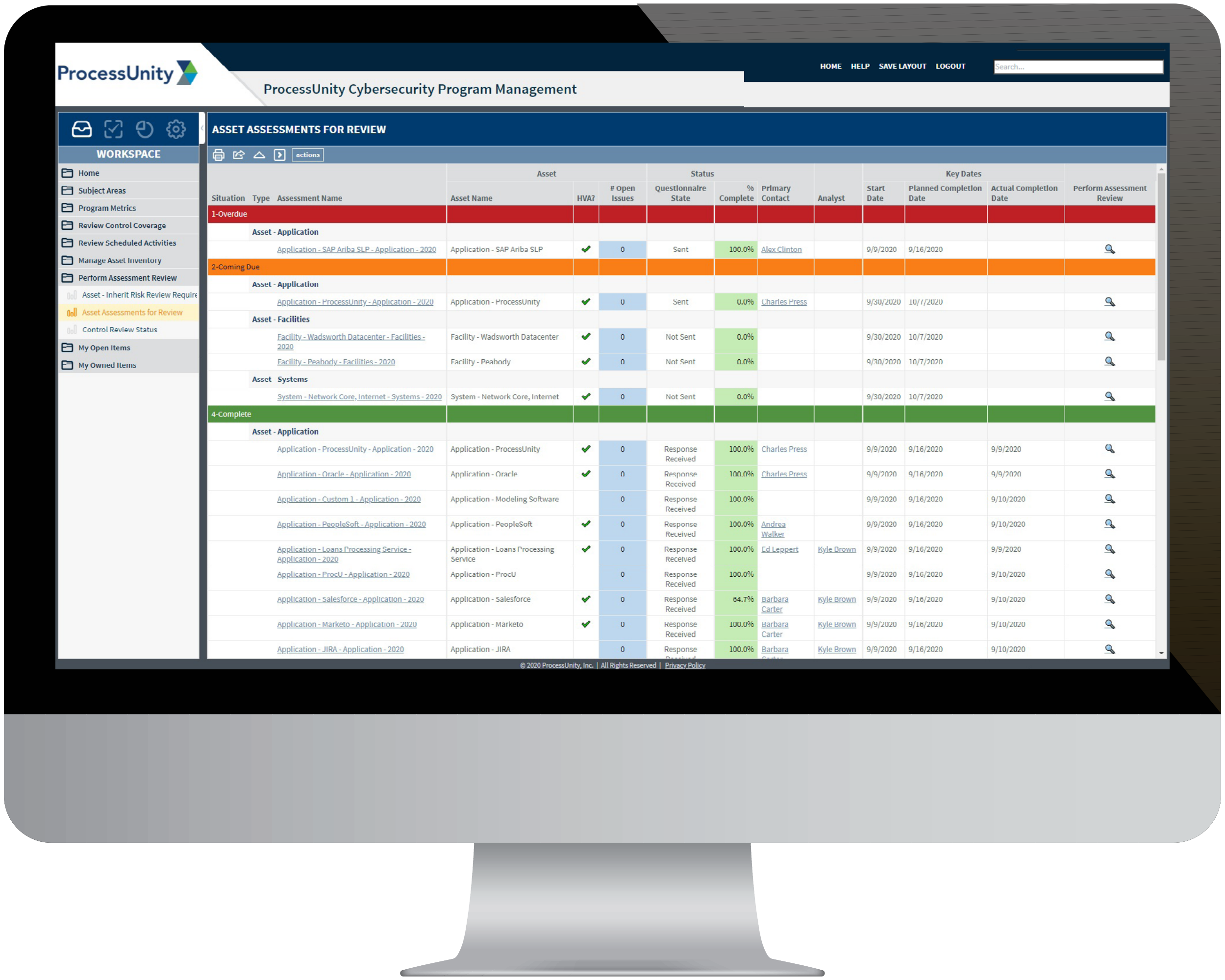
ASSET ASSESSMENTS FOR REVIEW REPORT

What is it?

The Asset Assessments for Review Report displays all completed, upcoming and overdue assessments across your applications, facilities and systems. This report shows open issues, questionnaire status, those responsible for the review and dates related to each task.

Why do you need it?

This report is an example of the various types of reports individuals and teams may use to manage the program or a CISO may leverage to gain deeper insight into the state of asset assessments. Not only is the questionnaire status clearly documented but the percentage of completion for assessments in flight can help you gain better visibility into and control of the assessment process.



ProcessUnity Cybersecurity Program Management

ASSET ASSESSMENTS FOR REVIEW

			Asset			Status				Key Dates			
Situation	Type	Assessment Name	Asset Name	HVA?	# Open Issues	Questionnaire State	% Complete	Primary Contact	Analyst	Start Date	Planned Completion Date	Actual Completion Date	Perform Assessment Review
1-Overdue													
	Asset - Application												
		Application - SAP Ariba SLP - Application - 2020	Application - SAP Ariba SLP	✓	0	Sent	100.0%	Alex Clinton		9/9/2020	9/16/2020		🔍
2-Coming Due													
	Asset - Application												
		Application - ProcessUnity - Application - 2020	Application - ProcessUnity	✓	0	Sent	0.0%	Charles Press		9/30/2020	10/7/2020		🔍
	Asset - Facilities												
		Facility - Wadsworth Datacenter - Facilities - 2020	Facility - Wadsworth Datacenter	✓	0	Not Sent	0.0%			9/30/2020	10/7/2020		🔍
		Facility - Peabody - Facilities - 2020	Facility - Peabody	✓	0	Not Sent	0.0%			9/30/2020	10/7/2020		🔍
	Asset Systems												
		System - Network Core, Internet - Systems - 2020	System - Network Core, Internet	✓	0	Not Sent	0.0%			9/30/2020	10/7/2020		🔍
4-Complete													
	Asset - Application												
		Application - ProcessUnity - Application - 2020	Application - ProcessUnity	✓	0	Response Received	100.0%	Charles Press		9/9/2020	9/16/2020	9/9/2020	🔍
		Application - Oracle - Application - 2020	Application - Oracle	✓	0	Response Received	100.0%	Charles Press		9/9/2020	9/16/2020	9/9/2020	🔍
		Application - Custom 1 - Application - 2020	Application - Modeling Software		0	Response Received	100.0%			9/9/2020	9/16/2020	9/10/2020	🔍
		Application - PeopleSoft - Application - 2020	Application - PeopleSoft	✓	0	Response Received	100.0%	Andrea Walker		9/9/2020	9/16/2020	9/10/2020	🔍
		Application - Loans Processing Service - Application - 2020	Application - Loans Processing Service	✓	0	Response Received	100.0%	Ed Leppert	Kyle Brown	9/9/2020	9/16/2020	9/9/2020	🔍
		Application - ProcU - Application - 2020	Application - ProcU		0	Response Received	100.0%			9/9/2020	9/16/2020	9/10/2020	🔍
		Application - Salesforce - Application - 2020	Application - Salesforce	✓	0	Response Received	64.7%	Barbara Carter	Kyle Brown	9/9/2020	9/16/2020	9/10/2020	🔍
		Application - Marketo - Application - 2020	Application - Marketo	✓	0	Response Received	100.0%	Barbara Carter	Kyle Brown	9/9/2020	9/16/2020	9/10/2020	🔍
		Application - JIRA - Application - 2020	Application - JIRA		0	Response	100.0%	Barbara	Kyle Brown	9/9/2020	9/16/2020	9/10/2020	🔍

> Next *Risk and Threat Dashboard*

ProcessUnity

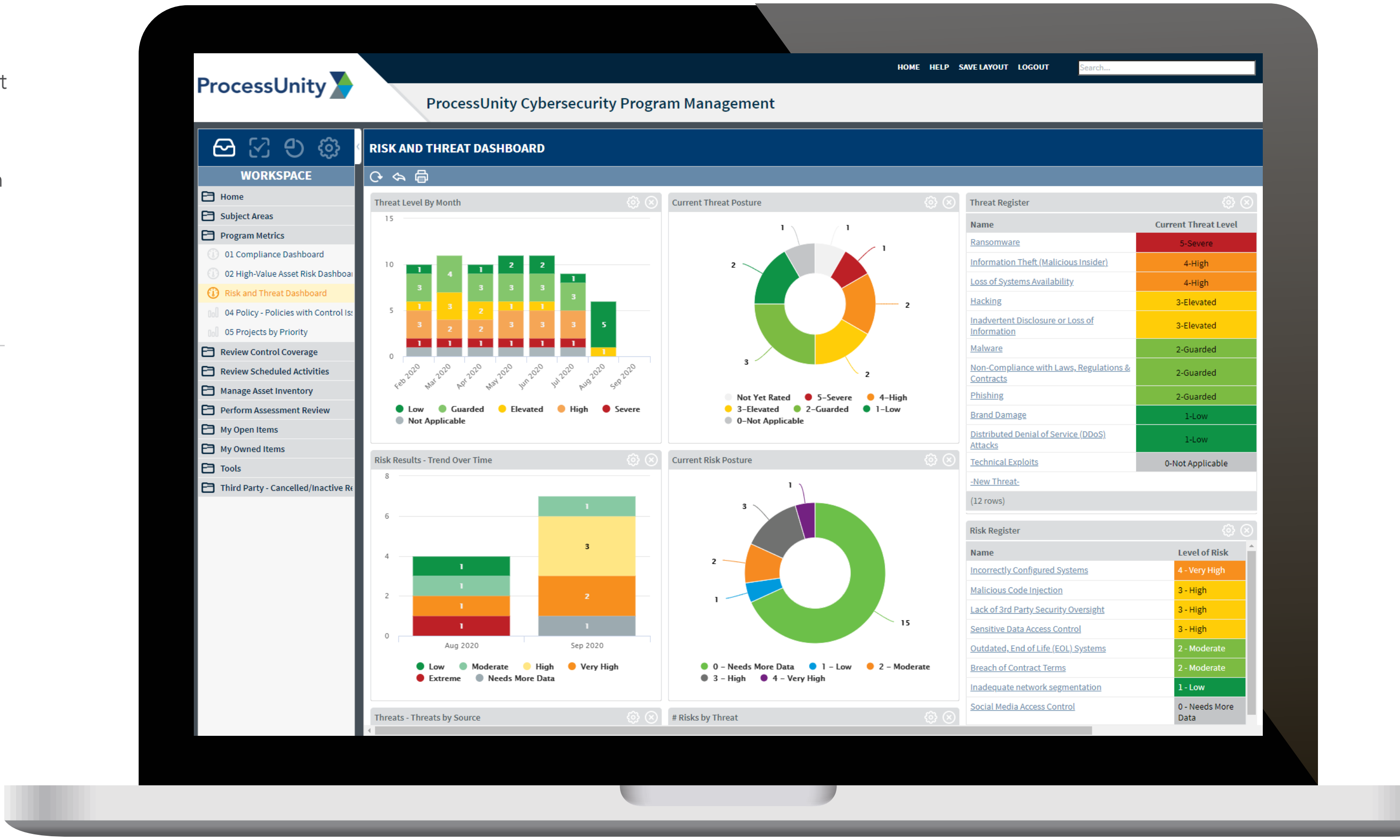
RISK AND THREAT DASHBOARD

What is it?

The Risk and Threat Dashboard shows your current threat posture, risks and threats by owner, threat level by month, risk results trending over time and risk and threat registers. These are presented from red to green to visually demonstrate the current level for each individual threat and risk identified and tracked in your cybersecurity program.

Why do you need it?

Knowing the current threat and risk level is critical to understanding where you stand today and what threats and risks need immediate attention. Trending information in this dashboard can demonstrate how your program is performing over time and reveal actionable insights into your threat and risk-related activities.



ProcessUnity

HOME HELP SAVE LAYOUT LOGOUT

ProcessUnity Cybersecurity Program Management

WORKSPACE

- Home
- Subject Areas
- Program Metrics
  - 01 Compliance Dashboard
  - 02 High-Value Asset Risk Dashboa
  - Risk and Threat Dashboard
  - 04 Policy - Policies with Control Is
  - 05 Projects by Priority
- Review Control Coverage
- Review Scheduled Activities
- Manage Asset Inventory
- Perform Assessment Review
- My Open Items
- My Owned Items
- Tools
- Third Party - Cancelled/Inactive Re

RISK AND THREAT DASHBOARD

Threat Register

Name	Current Threat Level
Ransomware	5-Severe
Information Theft (Malicious Insider)	4-High
Loss of Systems Availability	4-High
Hacking	3-Elevated
Inadvertent Disclosure or Loss of Information	3-Elevated
Malware	2-Guarded
Non-Compliance with Laws, Regulations & Contracts	2-Guarded
Phishing	2-Guarded
Brand Damage	1-Low
Distributed Denial of Service (DDoS) Attacks	1-Low
Technical Exploits	0-Not Applicable
-New Threat-	

(12 rows)

Risk Register

Name	Level of Risk
Incorrectly Configured Systems	4 - Very High
Malicious Code Injection	3 - High
Lack of 3rd Party Security Oversight	3 - High
Sensitive Data Access Control	3 - High
Outdated, End of Life (EOL) Systems	2 - Moderate
Breach of Contract Terms	2 - Moderate
Inadequate network segmentation	1 - Low
Social Media Access Control	0 - Needs More Data

> Next *Reporting On Your Cybersecurity Management Program*

REPORTING ON YOUR CYBERSECURITY MANAGEMENT PROGRAM

You implement cybersecurity program management to gain visibility. The right reports provide insight, save your team time, help you prioritize projects and demonstrate to the executive team and board that your cybersecurity risk is under control.

The foundation for effective and efficient cybersecurity program management is solid reporting. Unfortunately for many organizations, the key reports outlined in the previous pages are difficult to create without a great deal of manual effort. **You need automated, interactive reports to achieve success. That's where ProcessUnity comes in.**

ProcessUnity Cybersecurity Program Management is a single, comprehensive platform for centrally managing an organization's entire cybersecurity program with prepackaged mapped content, automated workflows, assessments and dynamic reporting. The solution enables the CISO to inventory and assess high-value assets; map them to threats, risks, policies and control standards; automate reviews; and capture evidence of compliance — all on a predefined schedule.

The reports in this eBook are standard, out-of-the-box reports that are always up-to-date, accurate and only one click away. In addition to these reports, our platform includes dozens of pre-made reports, all designed to gain great visibility and control of your cybersecurity program. **This is why organizations as small as community banks and as large as Fortune 50 companies rely on ProcessUnity.**

> Next *Ready to Learn More?*

READY TO LEARN MORE?

Watch a five-minute demonstration or click here to contact us today.

View Video

ProcessUnity

33 Bradford Street Concord, MA 01742 | www.processunity.com | info@processunity.com | tel 978.451.7655