DATA SHEET

PROCESSUNITY CYBERSECURITY PROGRAM MANAGEMENT

Gain visibility into the state of cybersecurity across the organization

ProcessUnity

Introduction

As a CISO, you have greater responsibility — and accountability — than ever before. You need to know if your organization has the right controls in place to manage cybersecurity threats and risks across applications, systems, facilities and third parties. At the same time, you need to respond to cyber-related inquiries coming from every direction — auditors, examiners, customers, lines of business and more. While there are plenty of tools out there to track scans, logs, discrete assets and other data, none of them provides one-stop visibility into the state of cybersecurity risk across the organization.

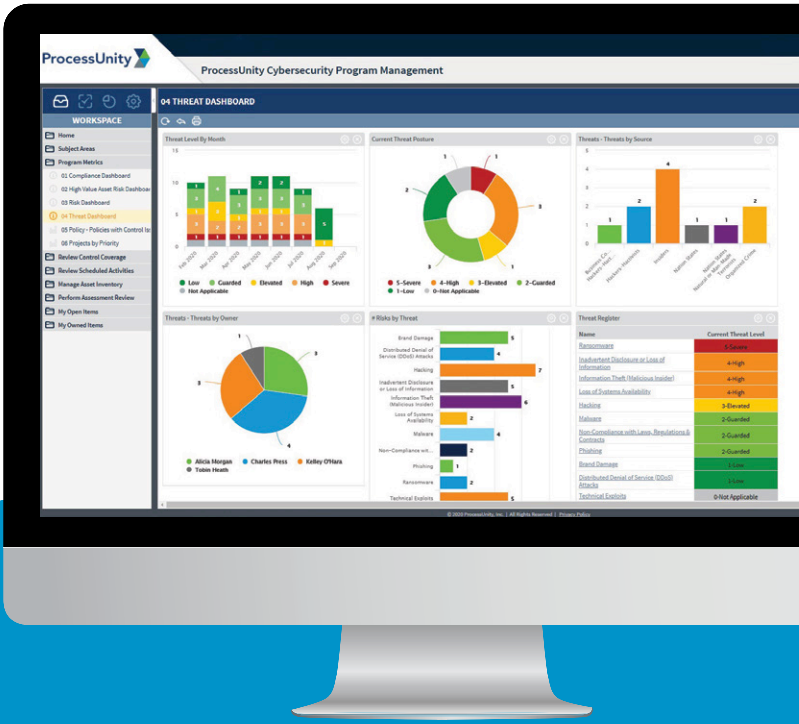
ProcessUnity Cybersecurity Program Management (CPM) is a single, comprehensive platform for centrally managing your entire cybersecurity program with prepackaged mapped content, automated workflows and assessments, and dynamic reporting. The system enables you to inventory and assess high-value assets; map them to threats, risks, policies and control standards; automate reviews; and capture evidence of compliance. It's never been easier to measure, react, and report on cyber-risk-related activities — on your preferred schedule — so you know exactly where you stand.

Designed specifically for the CISO, ProcessUnity CPM empowers you to create a risk-aware culture with a consistent, automated process for evaluating and remediating cybersecurity risk. The solution provides real-time access to the tools and metrics you need to prioritize your cyber projects, schedule your activities and prove your compliance. As a result, you're always prepared to communicate the impact of threats and risks to the executive team, risk committee and board of directors.

Key Benefits

- Get a complete, up-to-date view of your cybersecurity preparedness
- Identify and track cybersecurity-related projects across the organization
- Maintain one schedule for cyber reviews, assessments, remediation and training validation
- Monitor both internal and third-party assets in a single cybersecurity program
- Establish an answer bank of cybersecurity responses tied to a central control framework

Gain actionable insights to your threat-related activities and status via drill-down reports in the Threat Dashboard.



Threat Register

Name	Current Threat Level
Ransomware	5-Severe
Inadvertent Disclosure or Loss of Information	4-High
Information Theft (Malicious Insider)	4-High
Loss of Systems Availability	4-High
Hacking	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

Self-Configuring Control Framework & Schedule

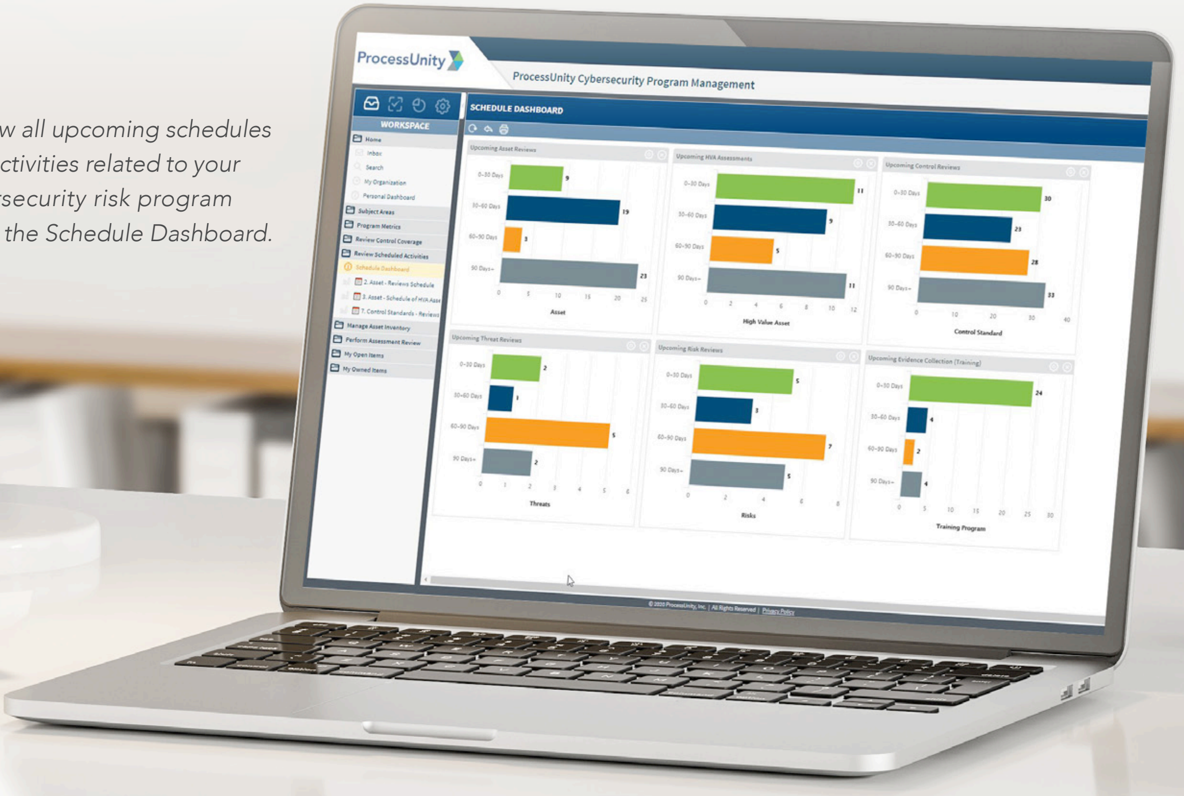
ProcessUnity's intelligent Cybersecurity Program Architect automatically scopes your program – mapping threats, risks, controls and regulations – via a step-by-step, guided self-assessment. The system self-configures an annual review schedule, complete with pre-built content, workflow triggers, notifications and reminders. Through hands-free automation, ProcessUnity CPM manages your program activities throughout the year, alerting stakeholders at appropriate times to make sure all tasks are completed, and all evidence is captured.

ProcessUnity leverages a pre-built meta model based on the Secure Controls Framework (SCF) mapped to the most common security frameworks, including NIST Cybersecurity Framework (CSF), NIST 800-53 and ISO 27002. The Cybersecurity Program Architect uses this meta model in combination with appropriate industry regulations (GDPR, CCPA, NYDFS, etc.) to intelligently select from a library of more than 800 supported control standards to ensure comprehensive coverage for your organization. You have the option to specify the cadences of cyber-related activities including threat, risk and control-rating reviews; assets and third-party assessments; and training program verification.

The scoping process culminates with the Cybersecurity Program Blueprint, a customized, board-ready report that presents your specific coverage recommendations, mapped threats, risks, controls, policies, program schedules and recommended next steps for continuous program improvement.

With your program foundation in place, ProcessUnity's configuration engine allows you to individualize your program – identifying assets, owners, and any additional threats, risks, controls and policies. This flexible and personalized configuration accelerates your deployment and time to value.

Review all upcoming schedules and activities related to your cybersecurity risk program using the Schedule Dashboard.

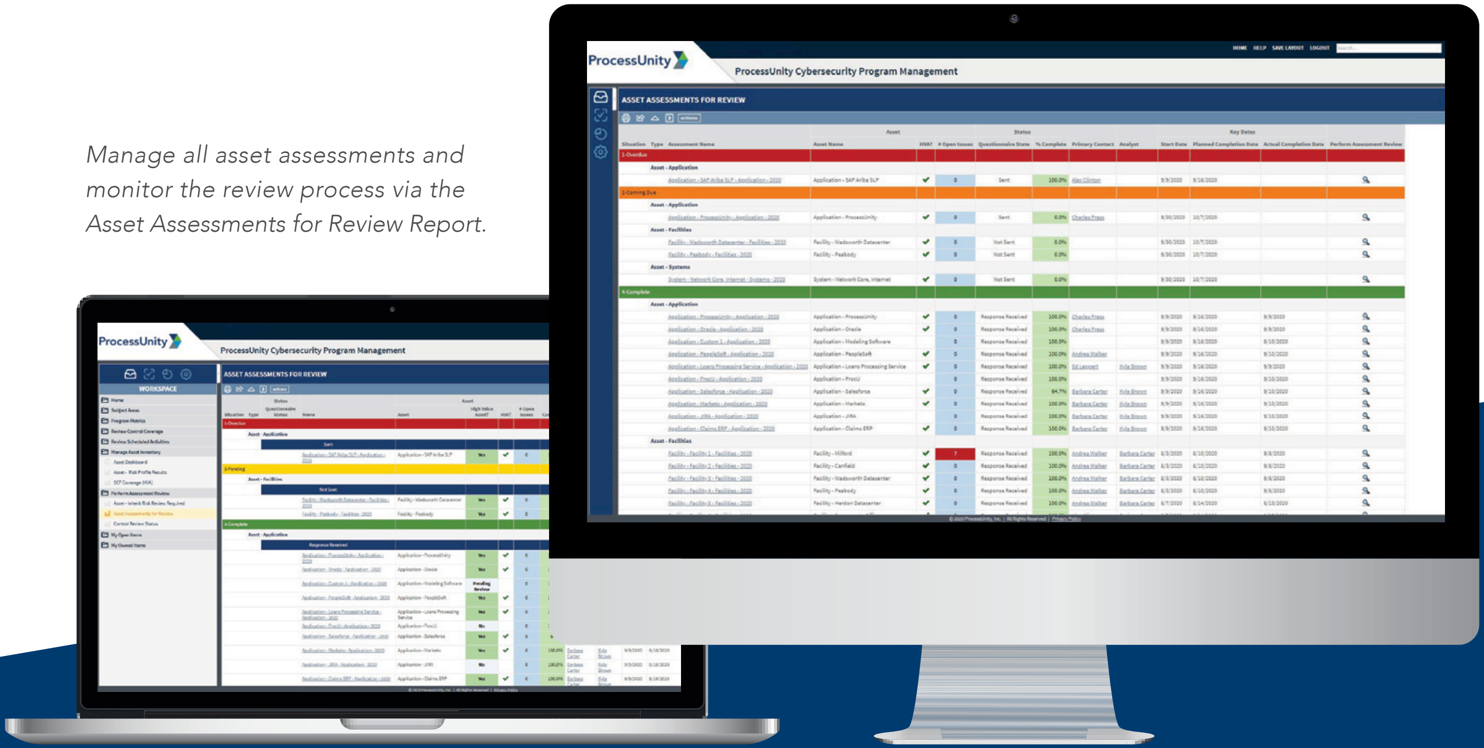


Automated Workflows & Assessments

Manage your cybersecurity program using a single, centralized platform instead of relying on a fragmented collection of disparate tools and appliances. ProcessUnity CPM provides automated workflows and assessments to make sure program activities stay on track throughout the year. The pre-built schedule triggers the automatic distribution of assessments and reviews to assigned stakeholders at the designated time — monitoring completion status and sending reminders when tasks are overdue.

ProcessUnity's workflow automation drives efficiency for scheduled program activities including:

- Threat Reviews
- Risk Evaluations
- Control Reviews
- Policy Reviews
- Incident Tracking
- Training Program Validation
- Issue Remediation
- Facility Assessment
- Application Assessment
- System Assessment
- Baseline Assessments



Manage all asset assessments and monitor the review process via the Asset Assessments for Review Report.

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 Received	100.0%	Barbara Carter	Kyle Brown	9/9/2020	9/16/2020	9/10/2020	🔍
		Application - Claims ERP - Application - 2020	Application - Claims ERP	✓	0	Response Received	100.0%	Barbara Carter	Kyle Brown	9/9/2020	9/16/2020	9/10/2020	🔍
	Asset - Facilities												
		Facility - Facility 1 - Facilities - 2020	Facility - Milford	✓	7	Response Received	100.0%	Andrea Walker	Barbara Carter	8/3/2020	8/10/2020	9/8/2020	🔍
		Facility - Facility 2 - Facilities - 2020	Facility - Canfield	✓	0	Response Received	100.0%	Andrea Walker	Barbara Carter	8/3/2020	8/10/2020	9/8/2020	🔍
		Facility - Facility 3 - Facilities - 2020	Facility - Wadsworth Datacenter	✓	0	Response Received	100.0%	Andrea Walker	Barbara Carter	8/3/2020	8/10/2020	9/8/2020	🔍
		Facility - Facility 4 - Facilities - 2020	Facility - Peabody	✓	0	Response Received	100.0%	Andrea Walker	Barbara Carter	8/3/2020	8/10/2020	9/8/2020	🔍
		Facility - Facility 5 - Facilities - 2020	Facility - Herdon Datacenter	✓	0	Response Received	100.0%	Andrea Walker	Barbara Carter	8/7/2020	8/14/2020	8/13/2020	🔍

© 2020 ProcessUnity, Inc. | All Rights Reserved | Privacy Policy

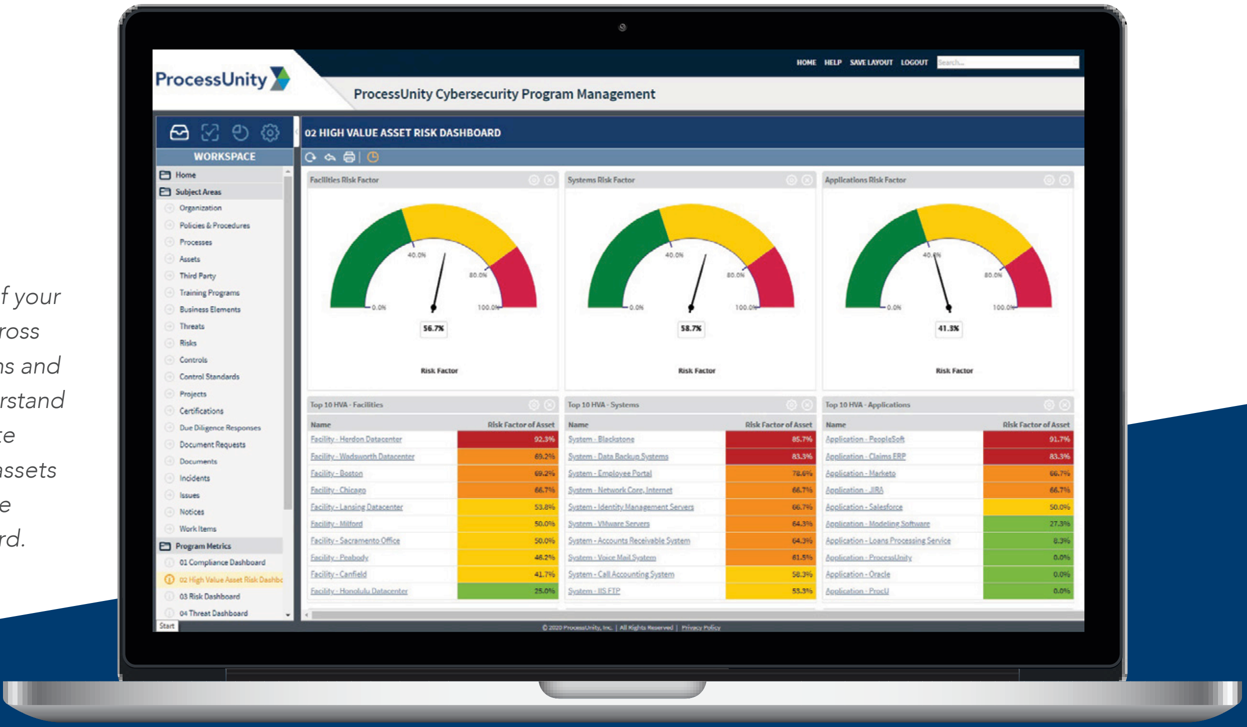
Interactive Dashboards & Reporting

ProcessUnity CPM's powerful reporting provides real-time visibility into the "state of the state" of your cybersecurity program. Interactive dashboards deliver at-a-glance insight into the level of threats, risks, policies, controls, issues and incidents enterprise-wide. Drill-down capabilities allow you to access details in areas of concern to prioritize investments and accelerate remediation.

Preconfigured reports track critical cybersecurity program data, including:

- Threat History & Trending
- Risk Remediation Status
- Policy Control Coverage
- Controls Effectiveness
- Risk Prioritized Projects
- Top High Value Assets at Risk
- Organizational Training Coverage
- Due Diligence Requests
- Top Third Parties at Risk
- Current Cyber Review Requests
- Issues Summary Status
- Major Incident Status

Extensive custom reporting capabilities allow you to create targeted reports and dashboards for the cybersecurity organization, C-suite, risk committee, the board of directors and others using an intuitive interface. With the click of a button, you can export a customized, real-time, board-level Word report on the state of the entire cybersecurity program – covering all relevant risks, threats, control reviews, assets, issues, incidents, projects and policies.



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%

Monitor the status of your high-value assets across your facilities, systems and applications to understand the state-of-the-state across your critical assets using the High-Value Asset Risk Dashboard.

Supported Program Activities

Whether supporting large teams or armies of one, ProcessUnity CPM manages all the activities that comprise a complete cybersecurity program. You can take advantage of all program components from day one, or you can activate functionality over time as your program evolves and matures.

Asset Management

What are your organization's Crown Jewels? ProcessUnity CPM makes it easy to import your assets —applications, systems, facilities, vendors, etc. — and assign owners. The system automatically sends an inherent risk assessment to each asset owner and scores responses to identify your high-value assets. Inherent risk ratings are used to determine your asset review schedule moving forward.

Threat Management

The threat landscape evolves constantly and you need to keep pace. With ProcessUnity CPM, you can evaluate and maintain a list of threats, their relevance and management's risk-tolerance level. The system triggers scheduled threat reviews, captures responses and evidence and automatically rolls up threat metrics and trends into the overall cybersecurity program status to guide strategic decisions.

Risk Management

Mitigating cybersecurity risk is your top priority. Use ProcessUnity CPM to identify, analyze, evaluate, treat and report on risk via a built-in risk register and pre-configured processes. The system triggers scheduled risk reviews and captures the data and evidence needed to substantiate risk likelihood and impact. Mapping identifies threat exposures associated with risks so you can deploy the right defenses.

Third-Party Cybersecurity Risk Management

Third-parties, vendors and suppliers are a key cybersecurity risk for any organization. ProcessUnity's Third-Party Cybersecurity Risk Management add-on lets you identify, monitor, and remediate cybersecurity risks posed by third parties over time. Pre-built questionnaires and workflows keep the assessment process moving on schedule. Third parties answer questions and attach documentation via a secure portal. The system tracks assessment status and sends alerts and notifications when follow-on actions are required.

Control Standards Inventory

When it comes to cybersecurity controls, it's your job to make sure you have all bases covered. ProcessUnity CPM tracks control effectiveness with a pre-loaded control framework aligned to key cybersecurity regulations and industry standards such as NIST and ISO. These control standards are also mapped to best-practice policies and assessments for clear line-of-sight risk and compliance assurance.

Organization & Training

People play a crucial role in your cybersecurity strategy. ProcessUnity CPM tracks relevant cybersecurity groups and manages ownership and accountability for threats, risks, controls, policies, assets, cyber training and projects, so you don't hit roadblocks due to personnel changes. The system also captures validation of required cybersecurity training and awareness programs.

Client Assurance

Don't let incoming due diligence requests bog down your cybersecurity experts. ProcessUnity CPM enables to organize, store and search a library of cybersecurity due diligence responses to speed and simplify client assurance activities. With a centralized repository of gold-master responses and supporting evidence, you can delegate due diligence requests to less expensive resources.

Policy Management

Today's cybersecurity challenges require accurate, up-to-date policies and practices. ProcessUnity CPM lets you store, maintain, review and certify formal policies and supporting processes/standards documents. The system links your policies to the control framework for synchronized compliance across the cybersecurity landscape. Whether a regulatory audit starts with a policy, or an asset assessment identifies a gap that ties back to a policy, you are covered for both transparency and impact.

Project Prioritizing

Program results help prioritize cybersecurity remediation projects for roadmap development. ProcessUnity CPM enables you to track and monitor key budgetary elements for each remediation project — and reassess upon completion to reduce organizational risk. Complete visibility into project status allows you to justify budgetary spend and keep business leaders informed.

Issue Management

Assessment processes identify issues that put your organization at risk. ProcessUnity CPM flags unacceptable responses that fall outside expectations, so you can create, manage, and analyze issues, making sure the assigned owner remediates to closure. The system supports multiple issues against a single asset and/or and multiple remediation plans against a single issue.

Measure. React. Report.

Say goodbye to limited cross-functional visibility and influence. ProcessUnity CPM provides a centralized system of record for managing cybersecurity activities across the organization. Combining a fully mapped control framework, automated workflows and best-practice assessments, the platform delivers comprehensive, accurate and on-time information to meet the evolving demands of cybersecurity governance, risk and compliance.

Interested in learning more?

Visit www.processunity.com/cybersecurity or contact us at info@processunity.com.

ProcessUnity

www.processunity.com

info@processunity.com

978.451.7655

Twitter: @processunity
LinkedIn: ProcessUnity

ProcessUnity
33 Bradford Street
Concord, MA 01742
United States