How to Build a Risk Register That Accounts for Internal and External Risk

IN THIS WEBINAR, YOU WILL LEARN HOW TO:

- CREATE A STRONG FOUNDATION FOR YOUR CYBER AND THIRD-PARTY RISK MANAGEMENT
- UNDERSTAND YOUR RISK LANDSCAPE THROUGH A HEATMAP
- DEVELOP ACTION PLANS FOR VULNERABILITIES IDENTIFIED IN YOUR RISK REGISTER

Brian Ventura

- 30+ years' IT experience, 10 years focused on CyberSecurity.
- SANS Certified Instructor
- IANS Faculty
- CISSP, GSLC, GCCC…

from the most trusted name in information security

Andrew Egoroff

- 25+ years' international experience providing cyber and cloud security advisory services
- Cybersecurity advisor for Process Unity's Cybersecurity Program Management (CPM) service offering
- CISSP, CCSP, CCSK, CISM, CRISC

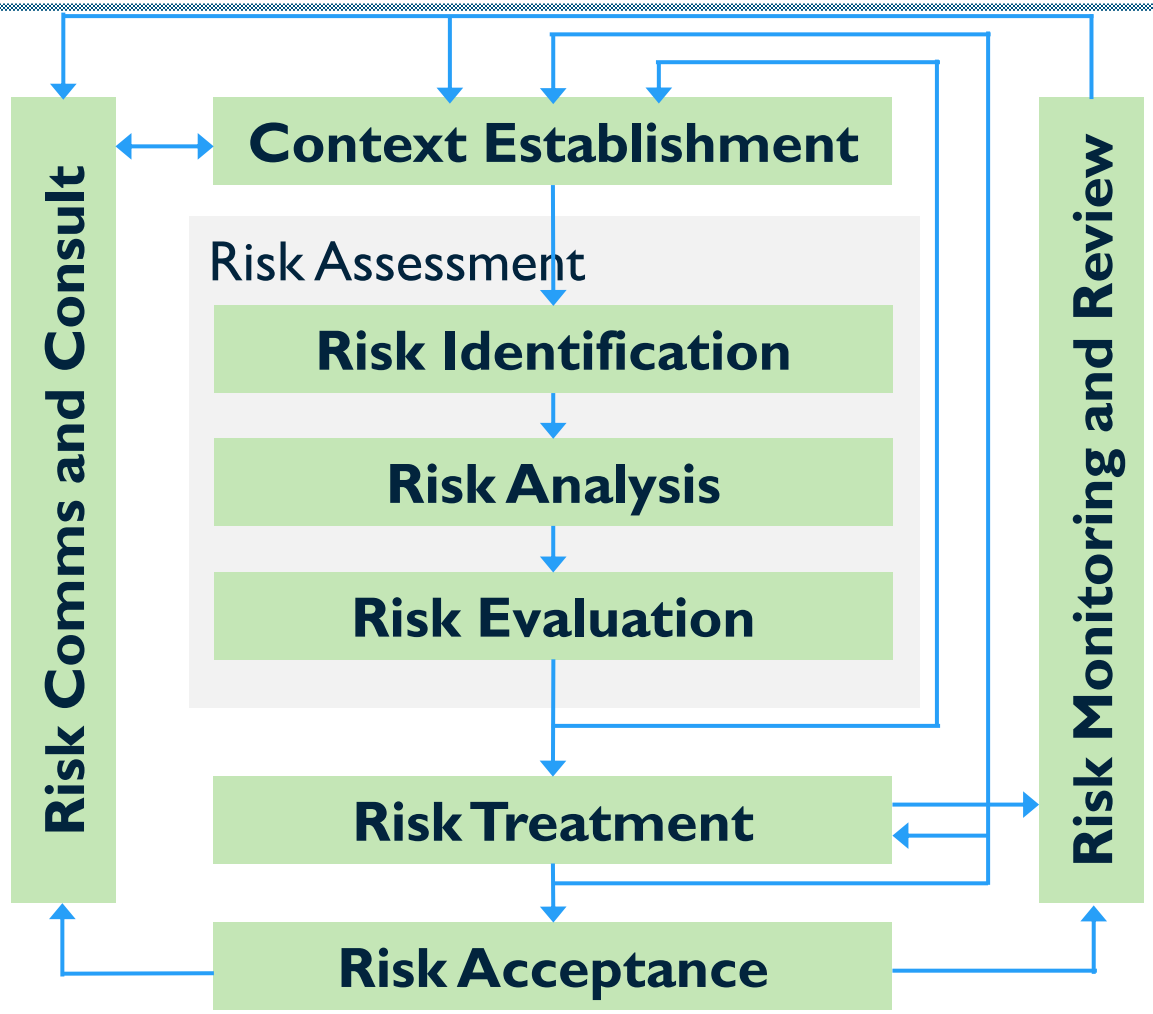
from the most trusted name in information security

Risk Overview

- Why measure risk?
- Assess risk
  - Risk Assessment for the purpose of Control Selection
  - Risk Assessment for the purpose of Gap Analysis
- Treat risk
  - Fix it now!
  - Accept risk
  - Plan/Budget for future work

Risk Assessment

- General risk assessment flow

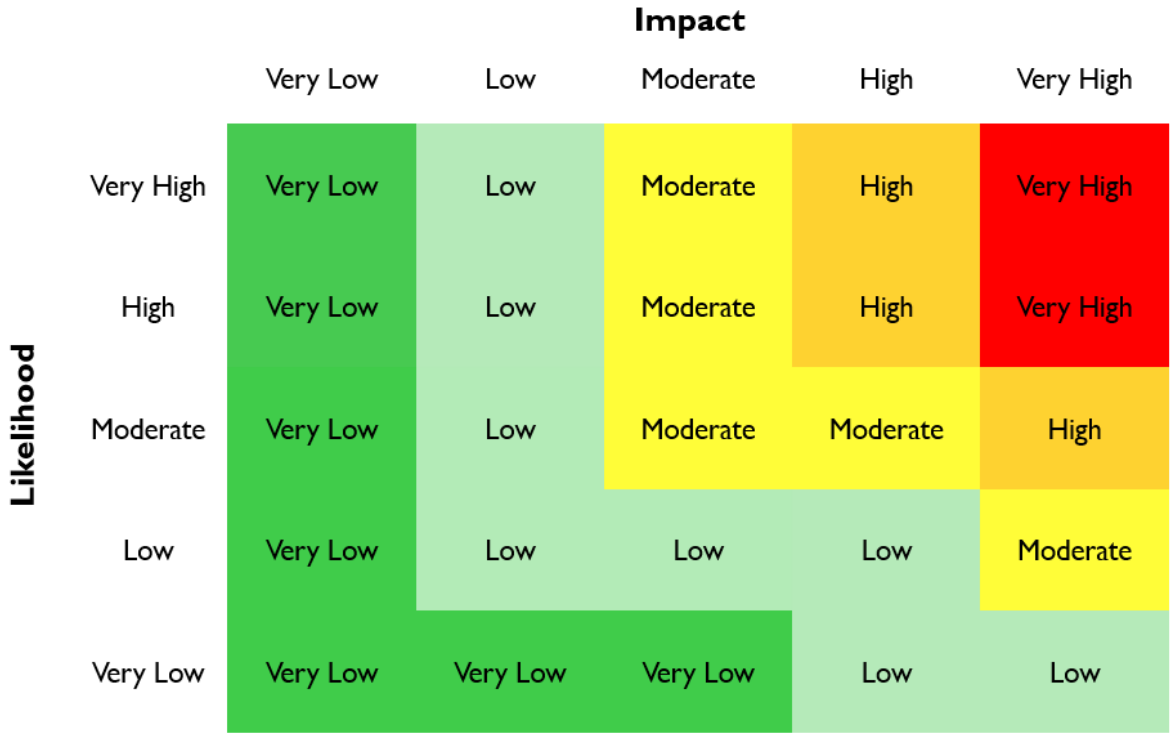


Internal risk and 3rd party risk

- 1st party risks – Directly address risk
  - Missing patch
  - Insecure communication
  - Insider threat
- 3rd party risks – Rely on 3rd party to address risk or stop doing business with 3rd party
  - Solarwinds
  - Log4Shell
  - Cloud / outsourced services

Qualitative risk prioritization

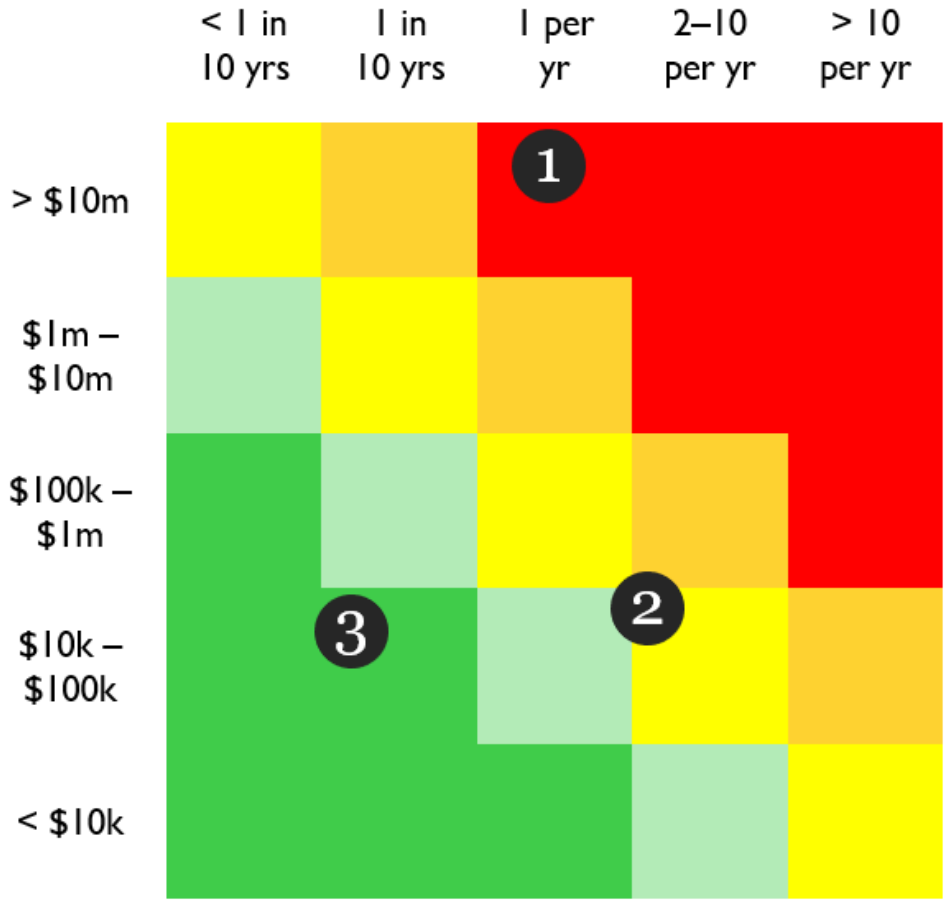
- Heat Map
  - Impact
  - Likelihood
- Calculate risk Level



Source: NIST 800-30 Table I-2

Quantitative and Qualitative

- Heat map shows qualitative
  - Quickly compare
- Quantitative risk overlaid
  - More specific understanding of risks



from the most trusted name in information security

Risk Register

- Track risks over time
  - Severity
  - Remediation plan/options
  - Budget requests
- Identify mitigations
- Prioritize risks
  - Qualitative - High, Medium, Low
  - Quantitative - $$

Risk Register - Example

- Spreadsheet example. Hard to track details

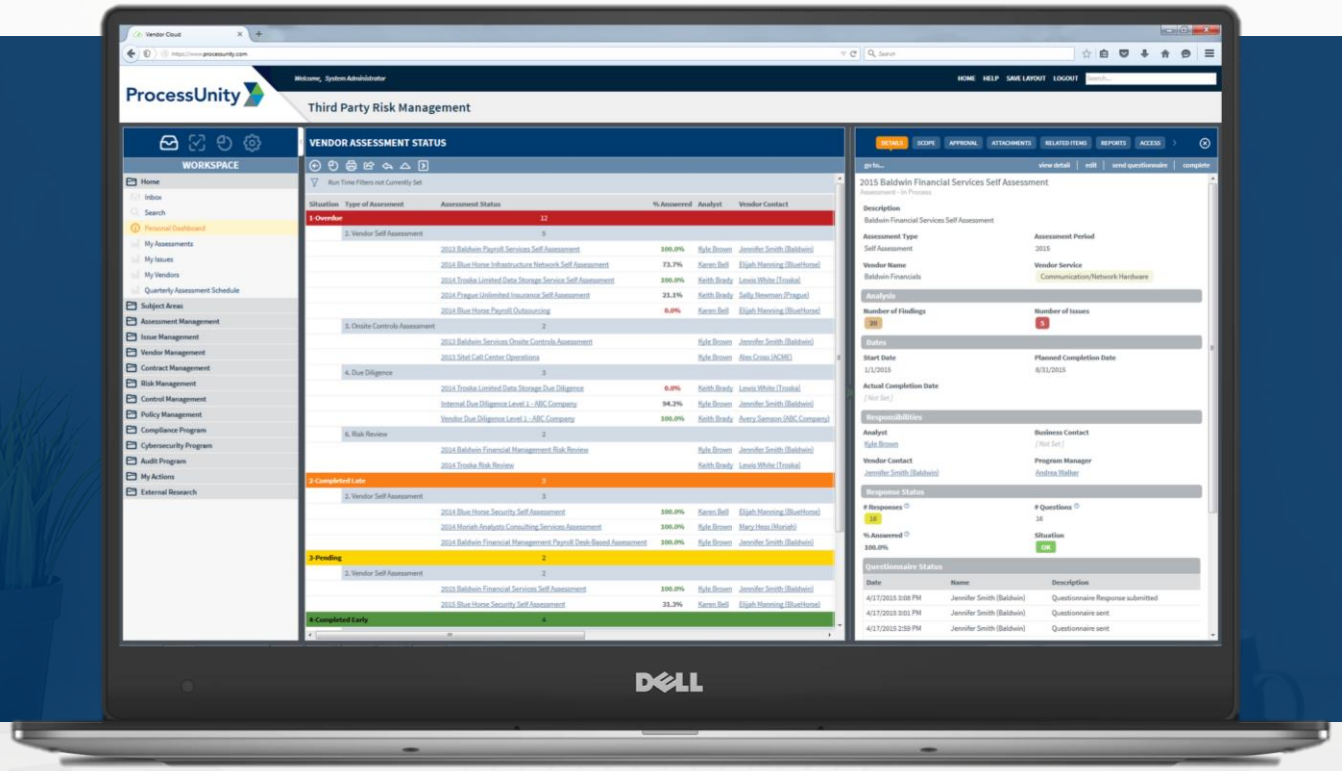
Description of Risk and Impact	Risk Owner	Impa	Likelih ood	Ratin	Mitigation	post mitigatio n Impa	mitigat ion Likel	Post mitigation rating
Missing patch on critical server, could cause a breach of sensitive data	Brian Ventura	5	4	20	Turned off external access to services	5	2	10
patch available. Could cause a breach	Sam Smith	5	5	25	????	5	5	25
broken, unauthorized access possible	Judy witt	5	3	15	Post guard 24x7	2	1	2
AV engine only detects signatures, System could be infected by 0day	Brian Ventura	3	3	9	Turn on EDR solutions	1	3	3
PCI data outside of cardholder environment may be exfiltrated	Betty Vice	5	4	20	Remove PCI data from non-cardholder systems and monitor for PCI information outside the environment	1	1	1

from the most trusted name in information security

ProcessUnity

Leader in Third-Party and Cybersecurity Risk Management Automation

The Top-Rated Third-Party & Cybersecurity Risk Management Platform



The Most Successful Customer Implementations in the Market

Pre-configured, content, workflows and processes

Unparalleled subject matter expertise

The shortest implementation times

Today’s Agenda

How to Build a Risk Register That Accounts for Internal and External Risk

- Create a strong foundation for your cyber and third-party risk management
- Understand your risk landscape through a heatmap
- Develop action plans for vulnerabilities identified in your risk register

Reliance on 3rd Parties and Supply Chains

3rd Party Risk – Something to be concerned about?

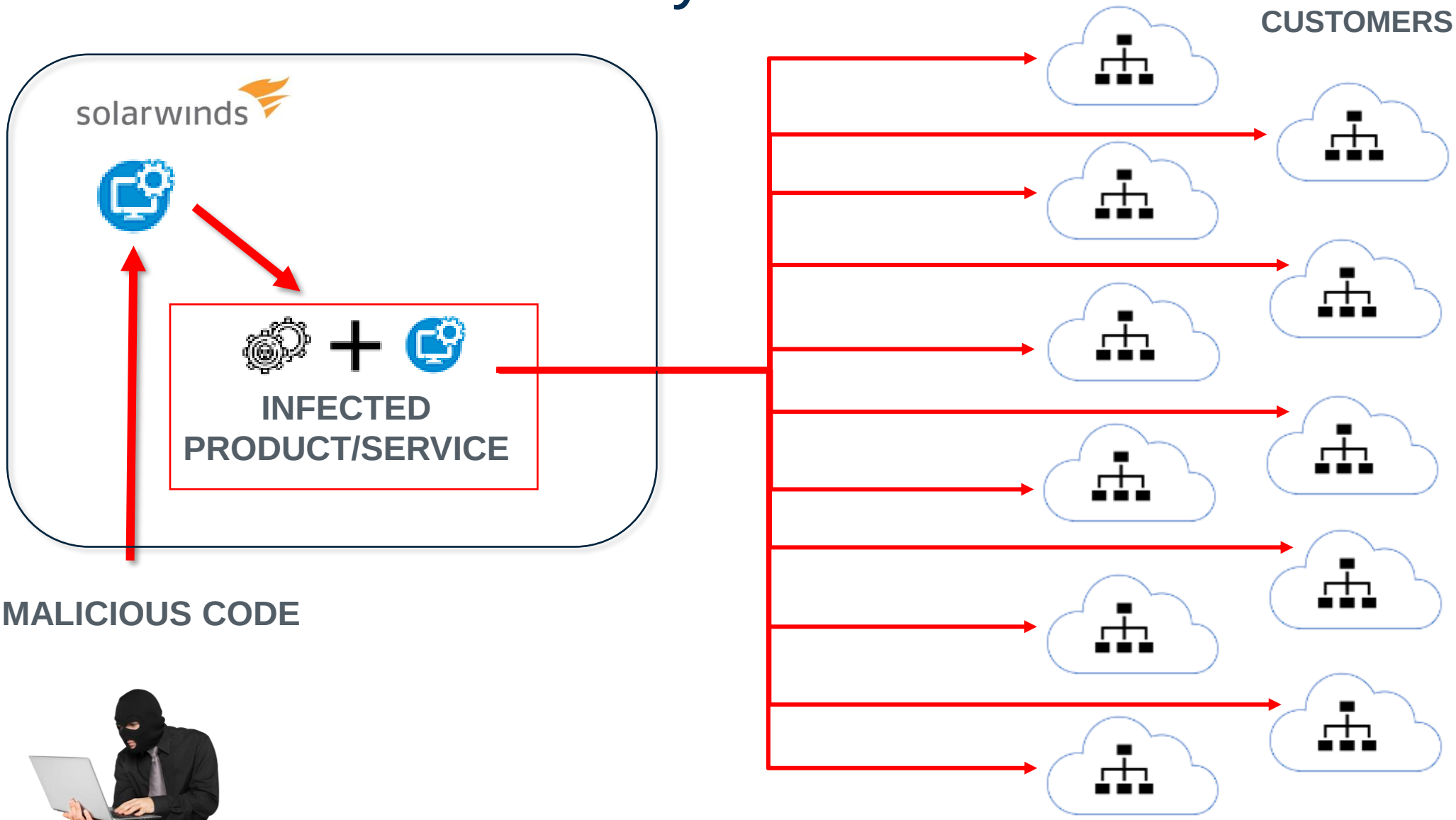
- PwC 2018: 63% of all cyber attacks can be traced to an organization third party (either directly or indirectly)[1]
- EY 2020: 35% of all organizations have experienced a data breach caused by a 3rd party[2]
- Deloitte 2021: More than half (51%) of organizations faced one or more third-party risk incident since March 2020[3]

[1] Rasner – Cybersecurity & Third-Party Risk

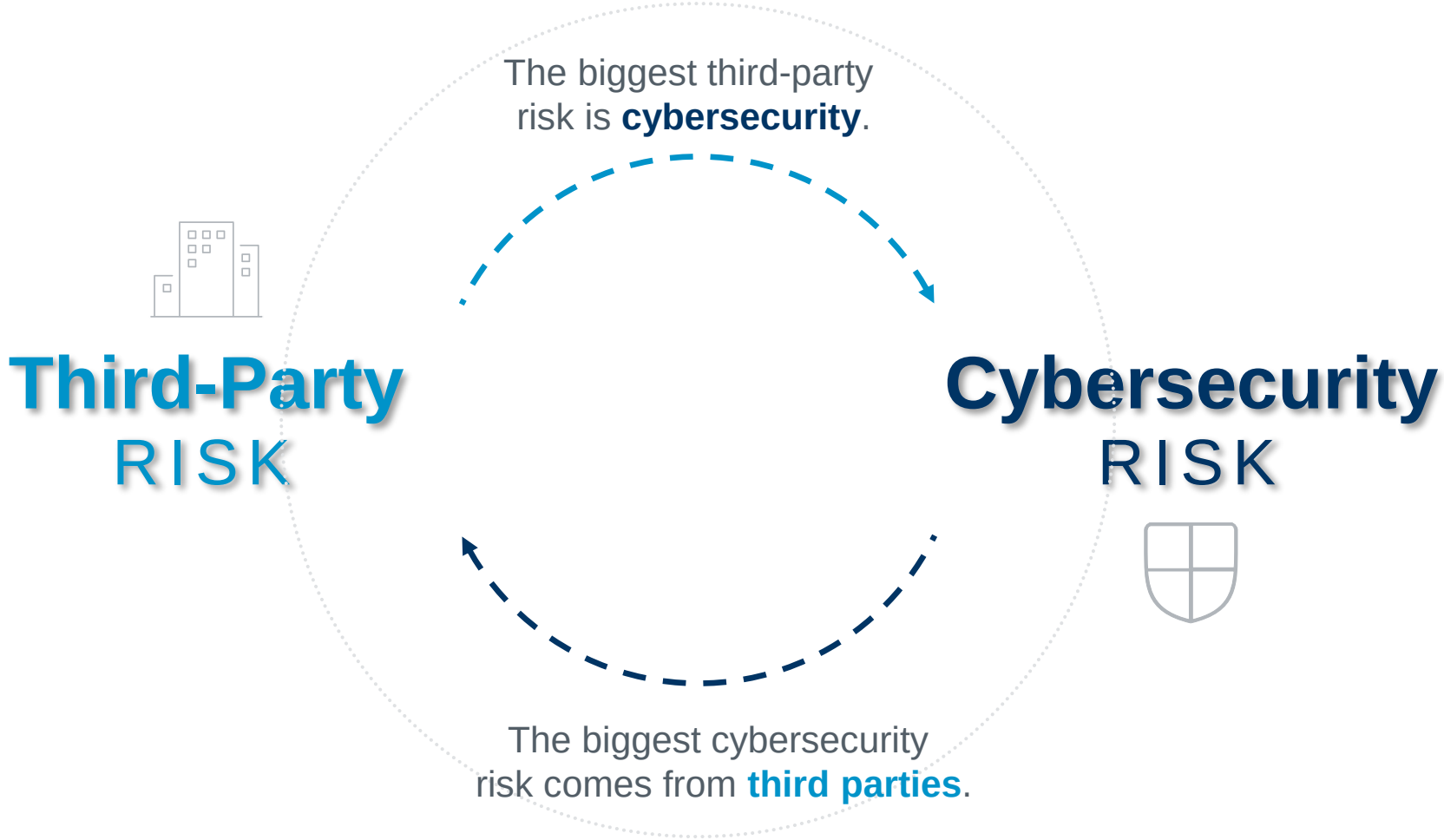
[2] EY Global Third-Party Risk Management Survey 2019-20

[3] Deloitte – TPRM Global Survey 2021

Sunburst Attack Analysis



The Biggest Risks Companies Face



The Biggest Risks Companies Face

"Treat your 3rd parties as an extension of your internal environment."

"Assess your 3rd parties' cybersecurity with the same set of controls as your internal environment."

MANAGING THIRD-PARTY & CYBER RISK

The Challenges

Top 5 Challenges

LACK OF VISIBILITY

INADEQUATE RISK ASSESSMENT

FRAGMENTED RISK MANAGEMENT

LIMITED COLLABORATION

NON-COMPLIANCE ISSUES

MANAGING THIRD-PARTY & CYBER RISK

The Solution

The Risk Register

FEATURES AND FUNCTIONS

The Risk Register

Risk Register – Key Features & Functions

- ✓ Centralized Repository
- ✓ Risk assessment and rating
- ✓ Mitigation tracking
- ✓ Stakeholder collaboration
- ✓ Reporting and analytics
- ✓ Integration with other systems
- ✓ Compliance support

The Risk Register

INCREASED VISIBILITY

IMPROVED RISK MANAGEMENT

WELL-INFORMED DECISION MAKING

ENHANCED COLLABORATION

COMPLIANCE SUPPORT

REAL-WORLD EXAMPLE

The Risk Register

WORKSPACE

Internal Control Assessments
Evidence Requests
Risks
Action Plans
Policies & Procedures
Policy Reviews
Issues
Documents

Enterprise Controls
Program Dashboard
A. Enterprise Controls
B. Control Assessments
C. Control Domain Ratings
D. Action Plan Tracker
E. Evidence Scheduler
F. Evidence Requests
G. Issue Tracker
H. Control Trend Analysis

Control Owner
A. My Control Tracker
B. My Control Reviews
C. My Open Issues

Evidence Collector
A. My Open Evidence Reque...

Enterprise Risks
Risk Dashboard
Risk's Methodology
A. Enterprise Risks
B. Heat Map
C. Risk Review Scheduler
D. Open Risk Reviews

Enterprise Policies

A. Enterprise Risks

Print | Export | Collapse All | TODAY 07:15 PM | Run Report

Risk Summary	Risk Category	Risks	Open Plan	Risk Description	Residual Risk	Risk Review			Inherent Risk			Last Review's Mitigating Factors			
					Severity	Last	Next	Open	Likelihood	Impact	Severity	CW	CM	MC	Other
Enterprise Risks			3	32				0							
	Access Control		2	4				0							
		Improper assignment of privileged functions	1	There is a failure to implement least privileges.	High	11/30/2022			Possible	Major	High	9.0	2.5	74	No Mitigating Factors Available
		Inability to maintain individual accountability	1	There is a failure to maintain asset ownership and it is not possible to have non-repudiation of actions or inactions.	Moderate	12/1/2022	12/2/2023		Highly Unlikely	Moderate	Moderate	8.9	2.5	76	Minimal Impact Reduction
		Privilege escalation		Access to privileged functions is inadequate or cannot be controlled.	Moderate	1/20/2023	1/20/2024		Highly Unlikely	Critical	Moderate	8.9	2.4	71	Minimal Impact Reduction
		Unauthorized access		Access is granted to unauthorized individuals, groups or services.	High	12/1/2022	6/1/2023		Unlikely	Critical	High	9.0	2.5	89	N/A - Not Required
	Asset Management		1	2				0							
		Loss of integrity through unauthorized changes	1	Unauthorized changes corrupt the integrity of the system / application / service.	Moderate	12/2/2022	6/2/2023		Possible	Moderate	High	9.0	2.4	88	Minimal Impact Reduction
		Lost, damaged or stolen asset(s)		Asset(s) is/are lost, damaged or stolen.	Moderate	11/23/2022	8/23/2023		Unlikely	Major	High	9.0	2.5	82	Minimal Impact Reduction
	Business Continuity		0	5				0							
		Business interruption		There is increased latency or a service outage that negatively impacts business operations.	High	11/23/2022	3/10/2023		Unlikely	Catastrophic	High	8.9	2.4	97	N/A - Not Required
		Data loss / corruption		There is a failure to maintain the confidentiality of the data (compromise) or data is corrupted (loss).	Moderate	1/23/2023	1/23/2024		Highly Unlikely	Critical	Moderate	8.9	2.4	97	No Mitigating Factors Available
		Information loss / corruption or system compromise due to non-technical attack		Social engineering, sabotage or other non-technical attack compromises data, systems, applications or services.	Moderate	11/23/2022	10/28/2023		Possible	Moderate	High	8.9	2.4	92	Moderate Impact Reduction
		Information loss / corruption or system compromise due to technical attack		Malware, phishing, hacking or other technical attack compromise data, systems, applications or services.	High	11/23/2022	4/23/2023		Almost Certain	Moderate	High	8.9	2.3	96	Minimal Impact Reduction
		Reduction in productivity		User productivity is negatively affected by the incident.	Moderate	11/23/2022	4/23/2023		Possible	Moderate	High	8.9	2.3	95	Minimal Impact Reduction
	Exposure		0	7				0							
		Cancelled contract		A contract is cancelled due to a violation of a contract clause.	Moderate	11/23/2022	4/23/2023		Remote	Catastrophic	Moderate	8.7	2.4	109	Minimal Impact Reduction
		Diminished competitive advantage		The competitive advantage of the organization is jeopardized.	Low	11/28/2022	3/28/2023		Remote	Insignificant	High	8.7	2.4	106	N/A - Not Required
		Diminished reputation		Negative publicity tarnishes the organization's reputation.	High	11/23/2022	6/23/2023		Unlikely	Catastrophic	High	8.8	2.4	107	N/A - Not Required
		Fines and judgements		Legal and/or financial damages result from statutory / regulatory / contractual non-compliance.	Moderate	11/23/2022	5/23/2023		Highly Unlikely	Moderate	Moderate	8.7	2.4	109	N/A - Not Required
		Loss of revenue		A financial loss occurs from either a loss of clients or an inability to generate future revenue.	Low	11/23/2022	1/23/2023		Highly Unlikely	Minor	Low	8.8	2.4	107	No Mitigating Factors Available
		System compromise		System / application / service is compromised affects its confidentiality, integrity, availability and/or safety.	High	11/23/2022	8/23/2023		Possible	Critical	Severe	9.0	2.4	88	Minimal Impact Reduction
				Unmitigated technical vulnerabilities exist without compensating											No Mitigating

WORKSPACE
ASSESSMENTS
REPORTS
SETTINGS
HELP

WORKSPACE
Internal Control Assessments
Evidence Requests
Risks
Action Plans
Policies & Procedures
Policy Reviews
Issues
Documents

Enterprise Controls
Program Dashboard
A. Enterprise Controls
B. Control Assessments
C. Control Domain Ratings
D. Action Plan Tracker
E. Evidence Scheduler
F. Evidence Requests
G. Issue Tracker
H. Control Trend Analysis

Control Owner
A. My Control Tracker
B. My Control Reviews
C. My Open Issues

Evidence Collector
A. My Open Evidence Reque...

Enterprise Risks
Risk Dashboard
Risk's Methodology
A. Enterprise Risks
B. Heat Map
C. Risk Review Scheduler
D. Open Risk Reviews

Enterprise Policies

A. Enterprise Risks

Print | Export | Collapse All | TODAY 07:15 PM | Run Report

Risk Summary	Risk Category	Risks	Open Plan	Risk Description	Residual Risk	Risk Review			Inherent Risk			Last Review's Mitigating Factors			
					Severity	Last	Next	Open	Likelihood	Impact	Severity	CW	CM	MC	Other
Enterprise Risks			3	32				0							
	Access Control		2	4				0							
		Improper assignment of privileged functions	1	There is a failure to implement least privileges.	High	11/30/2022			Possible	Major	High	9.0	2.5	74	No Mitigating Factors Available
		Inability to maintain individual accountability	1	There is a failure to maintain asset ownership and it is not possible to have non-repudiation of actions or inactions.	Moderate	12/1/2022	12/2/2023		Highly Unlikely	Moderate	Moderate	8.9	2.5	76	Minimal Impact Reduction
		Privilege escalation		Access to privileged functions is inadequate or cannot be controlled.	Moderate	1/20/2023	1/20/2024		Highly Unlikely	Critical	Moderate	8.9	2.4	71	Minimal Impact Reduction
		Unauthorized access		Access is granted to unauthorized individuals, groups or services.	High	12/1/2022	6/1/2023		Unlikely	Critical	High	9.0	2.5	89	N/A - Not Required
	Asset Management		1	2				0							
		Loss of integrity through unauthorized changes	1	Unauthorized changes corrupt the integrity of the system / application / service.	Moderate	12/2/2022	6/2/2023		Possible	Moderate	High	9.0	2.4	88	Minimal Impact Reduction
		Lost, damaged or stolen asset(s)		Asset(s) is/are lost, damaged or stolen.	Moderate	11/23/2022	8/23/2023		Unlikely	Major	High	9.0	2.5	82	Minimal Impact Reduction
	Business Continuity		0	5				0							
		Business interruption		There is increased latency or a service outage that negatively impacts business operations.	High	11/23/2022	3/10/2023		Unlikely	Catastrophic	High	8.9	2.4	97	N/A - Not Required
		Data loss / corruption		There is a failure to maintain the confidentiality of the data (compromise) or data is corrupted (loss).	Moderate	1/23/2023	1/23/2024		Highly Unlikely	Critical	Moderate	8.9	2.4	97	No Mitigating Factors Available
		Information loss / corruption or system compromise due to non-technical attack		Social engineering, sabotage or other non-technical attack compromises data, systems, applications or services.	Moderate	11/23/2022	10/28/2023		Possible	Moderate	High	8.9	2.4	92	Moderate Impact Reduction
		Information loss / corruption or system compromise due to technical attack		Malware, phishing, hacking or other technical attack compromise data, systems, applications or services.	High	11/23/2022	4/23/2023		Almost Certain	Moderate	High	8.9	2.3	96	Minimal Impact Reduction
		Reduction in productivity		User productivity is negatively affected by the incident.	Moderate	11/23/2022	4/23/2023		Possible	Moderate	High	8.9	2.3	95	Minimal Impact Reduction
	Exposure		0	7				0							
		Cancelled contract		A contract is cancelled due to a violation of a contract clause.	Moderate	11/23/2022	4/23/2023		Remote	Catastrophic	Moderate	8.7	2.4	109	Minimal Impact Reduction
		Diminished competitive advantage		The competitive advantage of the organization is jeopardized.	Low	11/28/2022	3/28/2023		Remote	Insignificant	High	8.7	2.4	106	N/A - Not Required
		Diminished reputation		Negative publicity tarnishes the organization's reputation.	High	11/23/2022	6/23/2023		Unlikely	Catastrophic	High	8.8	2.4	107	N/A - Not Required
		Fines and judgements		Legal and/or financial damages result from statutory / regulatory / contractual non-compliance.	Moderate	11/23/2022	5/23/2023		Highly Unlikely	Moderate	Moderate	8.7	2.4	109	N/A - Not Required
		Loss of revenue		A financial loss occurs from either a loss of clients or an inability to generate future revenue.	Low	11/23/2022	1/23/2023		Highly Unlikely	Minor	Low	8.8	2.4	107	No Mitigating Factors Available
		System compromise		System / application / service is compromised affects its confidentiality, integrity, availability and/or safety.	High	11/23/2022	8/23/2023		Possible	Critical	Severe	9.0	2.4	88	Minimal Impact Reduction
				Unmitigated technical vulnerabilities exist without compensating											No Mitigating

HOME
WORKSPACE
ASSESSMENTS
REPORTS
SETTINGS
HELP

WORKSPACE

Internal Control Assessments
Evidence Requests
Risks
Action Plans
Policies & Procedures
Policy Reviews
Issues
Documents

Enterprise Controls
Program Dashboard
A. Enterprise Controls
B. Control Assessments
C. Control Domain Ratings
D. Action Plan Tracker
E. Evidence Scheduler
F. Evidence Requests
G. Issue Tracker
H. Control Trend Analysis

Control Owner
A. My Control Tracker
B. My Control Reviews
C. My Open Issues

Evidence Collector
A. My Open Evidence Reque...

Enterprise Risks
Risk Dashboard
Risk's Methodology
A. Enterprise Risks
B. Heat Map
C. Risk Review Scheduler
D. Open Risk Reviews

Enterprise Policies

A. Enterprise Risks

Print | Export | Collapse All | TODAY 08:09 PM | Run Report

Risk Summary	Risk Category	Risks	Open Plan	Risk Description
Enterprise Risks			3	32
	Access Control		2	4
		Improper assignment of privileged functions	1	There is a failure to implement least privileges.
		Inability to maintain individual accountability	1	There is a failure to maintain asset ownership and it is not possib have non-repudiation of actions or inactions.
		Privilege escalation		Access to privileged functions is inadequate or cannot be control
		Unauthorized access		Access is granted to unauthorized individuals, groups or services
	Asset Management		1	2
		Loss of integrity through unauthorized changes	1	Unauthorized changes corrupt the integrity of the system / application / service.
		Lost, damaged or stolen asset(s)		Asset(s) is/are lost, damaged or stolen.
	Business Continuity		0	5
		Business interruption		There is increased latency or a service outage that negatively im business operations.
		Data loss / corruption		There is a failure to maintain the confidentiality of the data (compromise) or data is corrupted (loss).
		Information loss / corruption or system compromise due to non-technical attack		Social engineering, sabotage or other non-technical attack compromises data, systems, applications or services.
		Information loss / corruption or system compromise due to technical attack		Malware, phishing, hacking or other technical attack compromise data, systems, applications or services.
		Reduction in productivity		User productivity is negatively affected by the incident.
	Exposure		0	7
		Cancelled contract		A contract is cancelled due to a violation of a contract clause.
		Diminished competitive advantage		The competitive advantage of the organization is jeopardized.
		Diminished reputation		Negative publicity tarnishes the organization's reputation.
		Fines and judgements		Legal and/or financial damages result from statutory / regulatory contractual non-compliance.
		Loss of revenue		A financial loss occurs from either a loss of clients or an inability generate future revenue.
		System compromise		System / application / service is compromised affects its confidentiality, integrity, availability and/or safety.

Improper assignment of privileged functions

Risk

Details | Risk Reviews | Attachments | Related Items | Reports | Access | Change Log

Navigate To | Create Risk Review | Edit

Risk

Inherent Risk Severity (Helper)
3. High

Residual Risk Severity (Helper)
3. High

Inherent Risk Severity
3. High

Residual Risk Severity
3. High

Risk Manager
Rachel Miller

Risk Owner
Ryan Owens

Open Risk Reviews
0

Completed Risk Reviews
2

Open Action Plans
1

Completed Action Plans
0

Risk Description
There is a failure to implement least privileges.

Risk Scheduler

Risk Review Frequency
5. Annually

Next Review
[Not Set]

Latest Risk Review

Last Review Sent
[Not Set]

Last Review Completed
11/30/2022

Latest Risk Review Recommendations
Based off the previous risk review's outcome of a high residual risk severity, the program's recomendations are to evaluate the efficiency of existing controls, develop and implement additional control mechanisms, and monitor the risk quarterly.

Risk Likelihood
4. Possible

Risk Impact
4. Major

Number of Mitigating Controls
74

Average Relative Control Weight
8.95

Average Control Maturity
2.54

Other Mitigating Factors
2. No Mitigating Factors Available

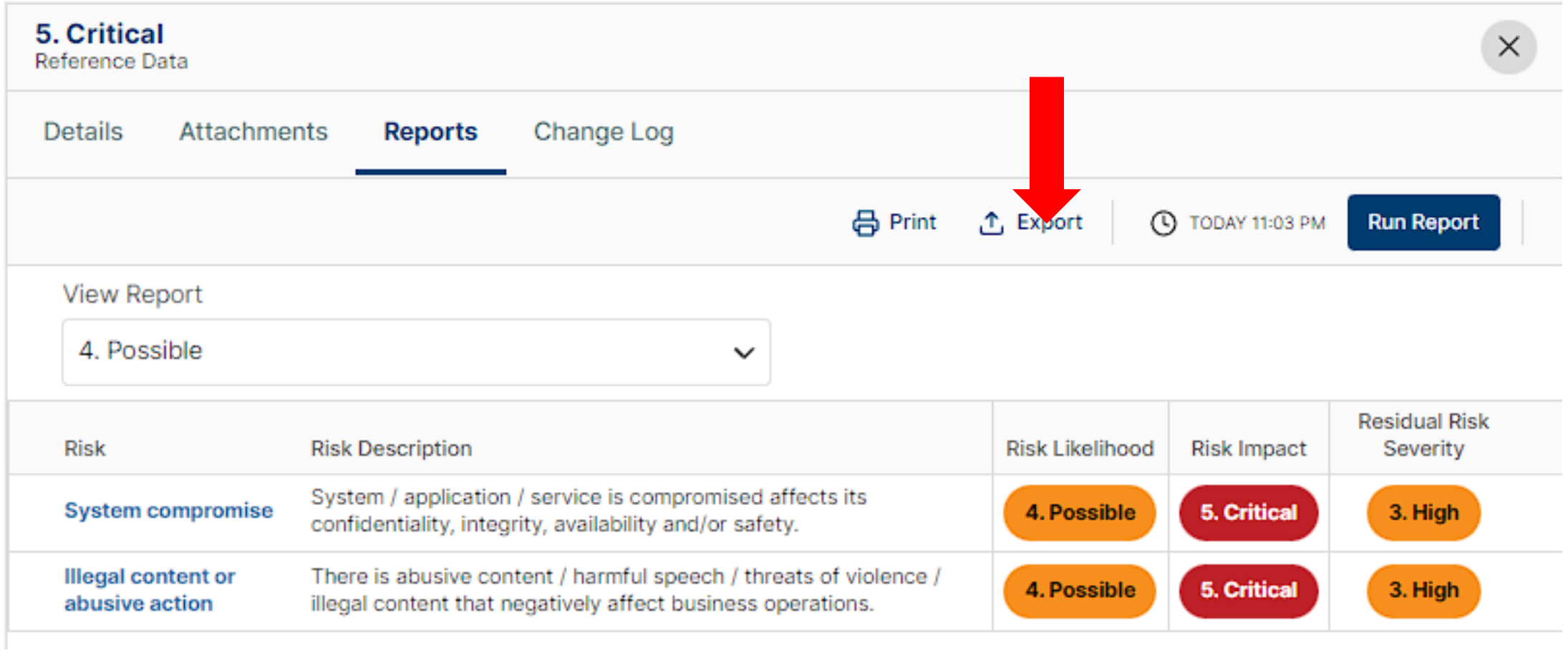
Other Mitigating Factors Description
no mitigating risk factors

Today’s Agenda

How to Build a Risk Register That Accounts for Internal and External Risk

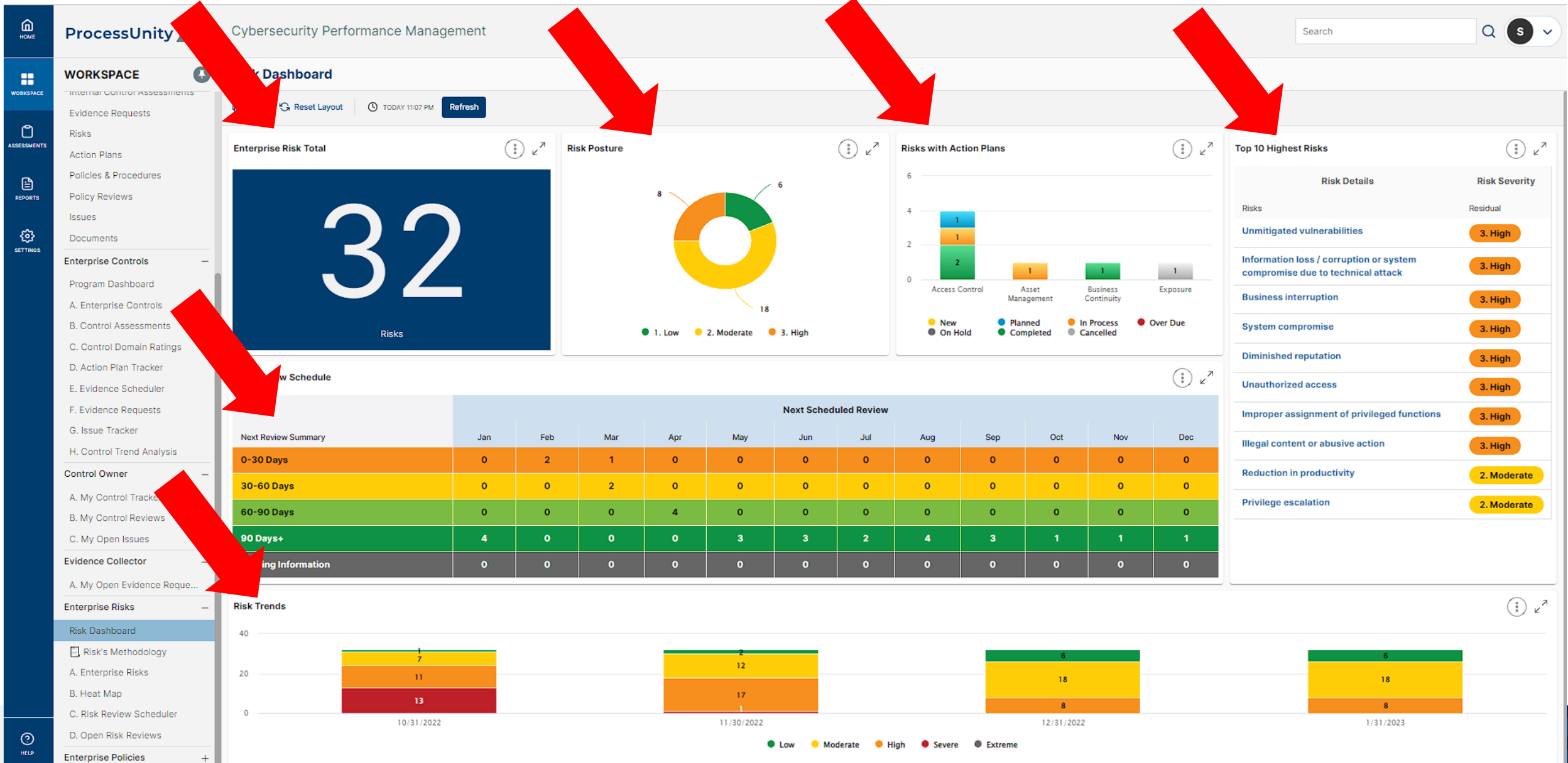
- Create a strong foundation for your cyber and third-party risk management
- Understand your risk landscape through a heatmap
- Develop action plans for vulnerabilities identified in your risk register

Heat Map



Risk	Risk Description	Risk Likelihood	Risk Impact	Residual Risk Severity
System compromise	System / application / service is compromised affects its confidentiality, integrity, availability and/or safety.	4. Possible	5. Critical	3. High
Illegal content or abusive action	There is abusive content / harmful speech / threats of violence / illegal content that negatively affect business operations.	4. Possible	5. Critical	3. High

Reporting & Analytics

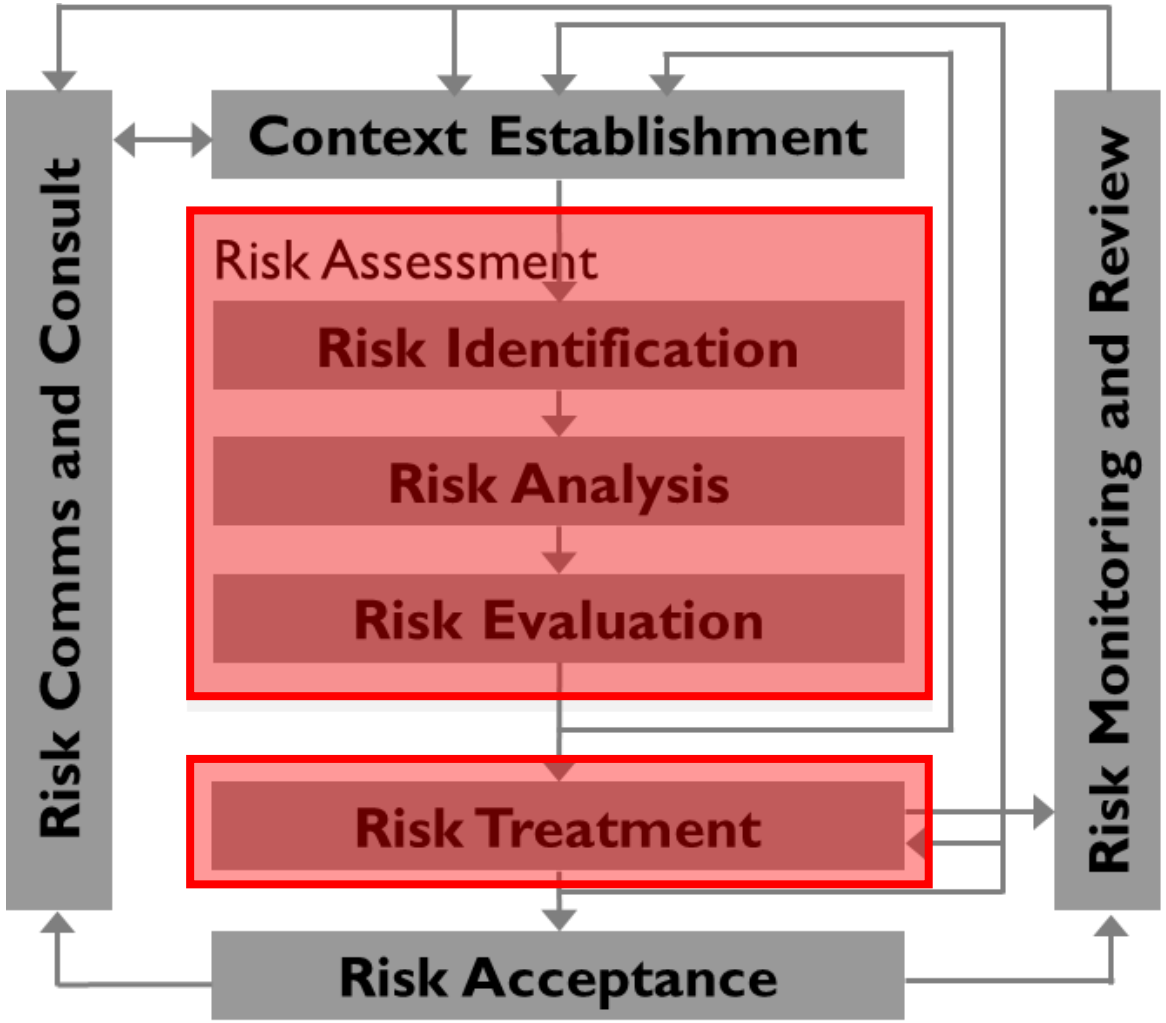


Today’s Agenda

How to Build a Risk Register That Accounts for Internal and External Risk

- Create a strong foundation for your cyber and third-party risk management
- Understand your risk landscape through a heatmap
- Develop action plans for vulnerabilities identified in your risk register

Risk Management



Action Plans

A. Enterprise Risks

Print | Export | Collapse All | TODAY 03:45 PM | Run Report

Risk Summary	Risk Category	Risks	Open Plan	Risk Description	Residual Risk Severity	Risk Review Last	Risk Review Next	Risk Review Open	Inherent Risk Likelihood	Inherent Risk Impact	Inherent Risk Severity	Last Review's Mitigating Factors CW	CM	MC	Other
Enterprise Risks			**2**	**32**				**1**							
	Access Control		**1**	**4**				**1**							
		Improper assignment of privileged functions		There is a failure to implement least privileges.	High	11/30/2022		1	Possible	Major	High	9.0	2.5	74	No Mitigating Factors Available
		Inability to maintain individual accountability		There is a failure to maintain asset ownership and it is not possible to have non-repudiation of actions or inactions.	Moderate	1/30/2023	12/2/2023		Highly Unlikely	Moderate	Moderate	8.9	2.5	76	Minimal Impact Reduction
		Privilege escalation	1	Access to privileged functions is inadequate or cannot be controlled.	Moderate	2/15/2023	2/15/2024		Highly Unlikely	Critical	Moderate	8.9	2.4	71	Minimal Impact Reduction
		Unauthorized access		Access is granted to unauthorized individuals, groups or services.	High	1/24/2023	1/24/2024		Unlikely	Critical	High	9.0	2.4	89	N/A - Not Required
	Asset Management		**1**	**2**				**0**							
		Loss of integrity through unauthorized changes	1	Unauthorized changes corrupt the integrity of the system / application / service.	Moderate	12/2/2022	6/2/2023		Possible	Moderate	High	9.0	2.4	88	Minimal Impact Reduction
		Lost, damaged or stolen asset(s)		Asset(s) is/are lost, damaged or stolen.	Moderate	11/23/2022	8/23/2023		Unlikely	Major	High	9.0	2.5	82	Minimal Impact Reduction
	Business Continuity		**0**	**5**				**0**							
		Business interruption		There is increased latency or a service outage that negatively impacts business operations.	High	11/23/2022	3/10/2023		Unlikely	Catastrophic	High	8.9	2.4	97	N/A - Not Required
		Data loss / corruption		There is a failure to maintain the confidentiality of the data (compromise) or data is corrupted (loss).	Moderate	1/23/2023	1/23/2024		Highly Unlikely	Critical	Moderate	8.9	2.4	97	No Mitigating Factors Available
		Information loss / corruption or system compromise due to non-technical attack		Social engineering, sabotage or other non-technical attack compromises data, systems, applications or services.	Moderate	11/23/2022	10/28/2023		Possible	Moderate	High	8.9	2.4	92	Moderate Impact Reduction
		Information loss / corruption or system compromise due to technical attack		Malware, phishing, hacking or other technical attack compromise data, systems, applications or services.	High	11/23/2022	4/23/2023		Almost Certain	Moderate	High	8.9	2.3	96	Minimal Impact Reduction
		Reduction in productivity		User productivity is negatively affected by the incident.	Moderate	11/23/2022	4/23/2023		Possible	Moderate	High	8.9	2.3	95	Minimal Impact Reduction
	Exposure		**0**	**7**				**0**							
		Cancelled contract		A contract is cancelled due to a violation of a contract clause.	Moderate	11/23/2022	4/23/2023		Remote	Catastrophic	Moderate	8.7	2.4	109	Minimal Impact Reduction
		Diminished competitive advantage		The competitive advantage of the organization is jeopardized.	Low	11/28/2022	3/28/2023		Remote	Insignificant	High	8.7	2.4	106	N/A - Not Required

A. Enterprise Risks

Print | Export | Collapse All | TODAY 03:45 PM | Run Report

Risk Summary	Risk Category	Risks	Open Plan	Risk Description
Enterprise Risks			**2**	**32**
	Access Control		**1**	**4**
		Improper assignment of privileged functions		There is a failure to implement least privileges.
		Inability to maintain individual accountability		There is a failure to maintain asset ownership and it is not possible non-repudiation of actions or inactions.
		Privilege escalation	1	Access to privileged functions is inadequate or cannot be controlle
		Unauthorized access		Access is granted to unauthorized individuals, groups or services.
	Asset Management		**1**	**2**
		Loss of integrity through unauthorized changes	1	Unauthorized changes corrupt the integrity of the system / applica service.
		Lost, damaged or stolen asset(s)		Asset(s) is/are lost, damaged or stolen.
	Business Continuity		**0**	**5**
		Business interruption		There is increased latency or a service outage that negatively impa business operations.
		Data loss / corruption		There is a failure to maintain the confidentiality of the data (compr data is corrupted (loss).
		Information loss / corruption or system compromise due to non-technical attack		Social engineering, sabotage or other non-technical attack compro data, systems, applications or services.
		Information loss / corruption or system compromise due to technical attack		Malware, phishing, hacking or other technical attack compromise c systems, applications or services.
		Reduction in productivity		User productivity is negatively affected by the incident.
	Exposure		**0**	**7**
		Cancelled contract		A contract is cancelled due to a violation of a contract clause.
		Diminished competitive advantage		The competitive advantage of the organization is jeopardized.

Unauthorized access

Risk

Details | Risk Assessments | Attachments | Related Items | Reports | Access | Change Log

Navigate To | Create Risk Assessment | Edit

Risk

Inherent Risk Severity
3. High

Residual Risk Severity
3. High

Risk Manager
Rachel Miller

Risk Owner
Ryan Owens

Open Risk Assessments
0

Completed Risk Assessments
3

Open Action Plans
0

Completed Action Plans
1

Risk Description
Access is granted to unauthorized individuals, groups or services.

Risk Scheduler

Risk Assessment Frequency
5. Annually

Next Risk Assessment
1/24/2024

Latest Risk Assessment

Last Risk Assessment Sent
1/24/2023

Last Risk Assessment Completed
1/24/2023

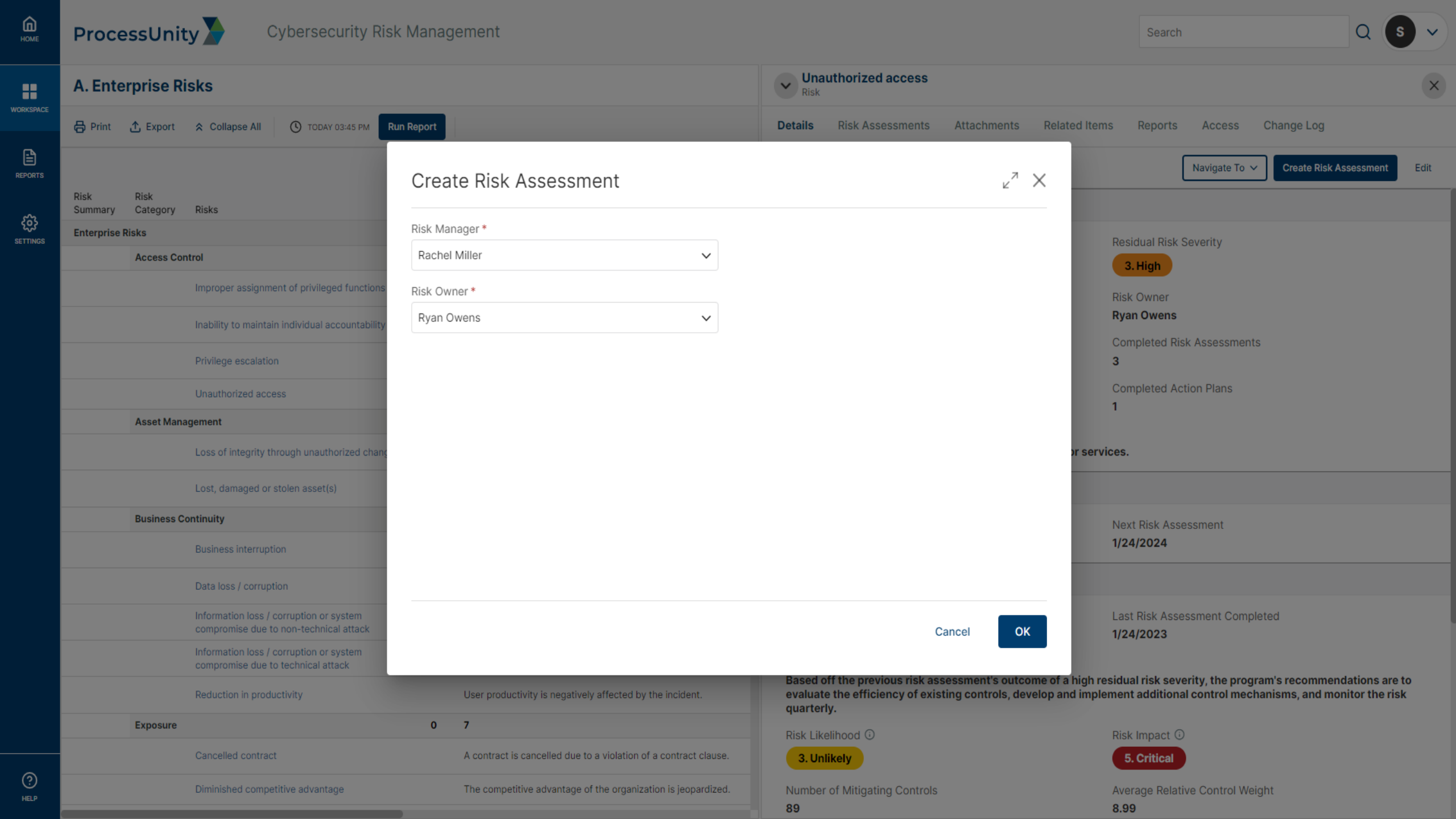
Latest Risk Assessment Recommendations
Based off the previous risk assessment's outcome of a high residual risk severity, the program's recommendations are to evaluate the efficiency of existing controls, develop and implement additional control mechanisms, and monitor the risk quarterly.

Risk Likelihood
3. Unlikely

Risk Impact
5. Critical

Number of Mitigating Controls
89

Average Relative Control Weight
8.99


ProcessUnity
Cybersecurity Risk Management
Search
HOME
WORKSPACE
REPORTS
SETTINGS
HELP
A. Enterprise Risks
Print
Export
Collapse All
TODAY 03:45 PM
Run Report
Risk Summary
Risk Category
Risks
Enterprise Risks
Access Control
Improper assignment of privileged functions
Inability to maintain individual accountability
Privilege escalation
Unauthorized access
Asset Management
Loss of integrity through unauthorized chang
Lost, damaged or stolen asset(s)
Business Continuity
Business interruption
Data loss / corruption
Information loss / corruption or system compromise due to non-technical attack
Information loss / corruption or system compromise due to technical attack
Reduction in productivity
User productivity is negatively affected by the incident.
Exposure
0
7
Cancelled contract
A contract is cancelled due to a violation of a contract clause.
Diminished competitive advantage
The competitive advantage of the organization is jeopardized.
Unauthorized access
Risk
Details
Risk Assessments
Attachments
Related Items
Reports
Access
Change Log
Navigate To
Create Risk Assessment
Edit
Residual Risk Severity
3. High
Risk Owner
Ryan Owens
Completed Risk Assessments
3
Completed Action Plans
1
or services.
Next Risk Assessment
1/24/2024
Last Risk Assessment Completed
1/24/2023
Based off the previous risk assessment's outcome of a high residual risk severity, the program's recommendations are to evaluate the efficiency of existing controls, develop and implement additional control mechanisms, and monitor the risk quarterly.
Risk Likelihood
3. Unlikely
Risk Impact
5. Critical
Number of Mitigating Controls
89
Average Relative Control Weight
8.99
Create Risk Assessment
Risk Manager *
Rachel Miller
Risk Owner *
Ryan Owens
Cancel
OK

A. Enterprise Risks

Print | Export | Collapse All | TODAY 03:45 PM | Run Report

Risk Summary	Risk Category	Risks	Open Plan	Risk Description
Enterprise Risks			**2**	**32**
	Access Control		**1**	**4**
		Improper assignment of privileged functions		There is a failure to implement least privileges.
		Inability to maintain individual accountability		There is a failure to maint… non-repudiation of action
		Privilege escalation	1	Access to privileged func…
		Unauthorized access		Access is granted to una…
	Asset Management		**1**	**2**
		Loss of integrity through unauthorized changes	1	Unauthorized changes co… service.
		Lost, damaged or stolen asset(s)		Asset(s) is/are lost, dama…
	Business Continuity		**0**	**5**
		Business interruption		There is increased latency or a service outage that negatively impa… business operations.
		Data loss / corruption		There is a failure to maintain the confidentiality of the data (compr… data is corrupted (loss).
		Information loss / corruption or system compromise due to non-technical attack		Social engineering, sabotage or other non-technical attack comprc… data, systems, applications or services.
		Information loss / corruption or system compromise due to technical attack		Malware, phishing, hacking or other technical attack compromise c… systems, applications or services.
		Reduction in productivity		User productivity is negatively affected by the incident.
	Exposure		**0**	**7**
		Cancelled contract		A contract is cancelled due to a violation of a contract clause.
		Diminished competitive advantage		The competitive advantage of the organization is jeopardized.

Unauthorized access

Risk

Details | Risk Assessments | Attachments | Related Items | Reports | Access | Change Log

Navigate To | Create Risk Assessment | Edit

Risk

Inherent Risk Severity
3. High

Residual Risk Severity
3. High

Risk Manager
Rachel Miller

Risk Owner
Ryan Owens

…ents

Completed Risk Assessments
3

Completed Action Plans
1

…o unauthorized individuals, groups or services.

Risk Assessment Frequency
5. Annually

Next Risk Assessment
1/24/2024

Latest Risk Assessment

Last Risk Assessment Sent
1/24/2023

Last Risk Assessment Completed
1/24/2023

Latest Risk Assessment Recommendations
Based off the previous risk assessment's outcome of a high residual risk severity, the program's recommendations are to evaluate the efficiency of existing controls, develop and implement additional control mechanisms, and monitor the risk quarterly.

Risk Likelihood
3. Unlikely

Risk Impact
5. Critical

Number of Mitigating Controls
89

Average Relative Control Weight
8.99

Confirm

Are you sure you want to create a risk assessment?

Cancel | OK

A. Enterprise Risks

Print | Export | Collapse All | TODAY 03:51 PM | Run Report

Risk Summary	Risk Category	Risks	Open Plan	Risk Description
Enterprise Risks			**2**	**32**
	Access Control		**1**	**4**
		Improper assignment of privileged functions		There is a failure to implement least privileges.
		Inability to maintain individual accountability		There is a failure to maintain asset ownership and it is not possible non-repudiation of actions or inactions.
		Privilege escalation	1	Access to privileged functions is inadequate or cannot be controlle
		Unauthorized access		Access is granted to unauthorized individuals, groups or services.
	Asset Management		**1**	**2**
		Loss of integrity through unauthorized changes	1	Unauthorized changes corrupt the integrity of the system / applica service.
		Lost, damaged or stolen asset(s)		Asset(s) is/are lost, damaged or stolen.
	Business Continuity		**0**	**5**
		Business interruption		There is increased latency or a service outage that negatively impa business operations.
		Data loss / corruption		There is a failure to maintain the confidentiality of the data (compr data is corrupted (loss).
		Information loss / corruption or system compromise due to non-technical attack		Social engineering, sabotage or other non-technical attack compro data, systems, applications or services.
		Information loss / corruption or system compromise due to technical attack		Malware, phishing, hacking or other technical attack compromise c systems, applications or services.
		Reduction in productivity		User productivity is negatively affected by the incident.
	Exposure		**0**	**7**
		Cancelled contract		A contract is cancelled due to a violation of a contract clause.
		Diminished competitive advantage		The competitive advantage of the organization is jeopardized.

Risk Assessment2023-02-17 - Unauthorized access

Risk Assessment

Details | Attachments | Related Items | Access | Change Log

Navigate To | Prepare Risk Assessment | Edit

Risk Assessment

Inherent Risk Severity
3. High

Residual Risk Severity
3. High

Assessment Status
1. Open

Parent Risk
Unauthorized access

Risk Manager
Rachel Miller

Risk Owner
Ryan Owens

Risk Description
Access is granted to unauthorized individuals, groups or services.

Risk Assessment Dates

Date 1 - Open
2/17/2023

Date 2 - In Progress
[Not Set]

Date 3 - Due
[Not Set]

Date 4 - Decision
[Not Set]

Date 5 - Complete
[Not Set]

Risk Assessment Completed By
[Not Set]

Risk Assessment Lifecycle in Business Days
[Not Set]

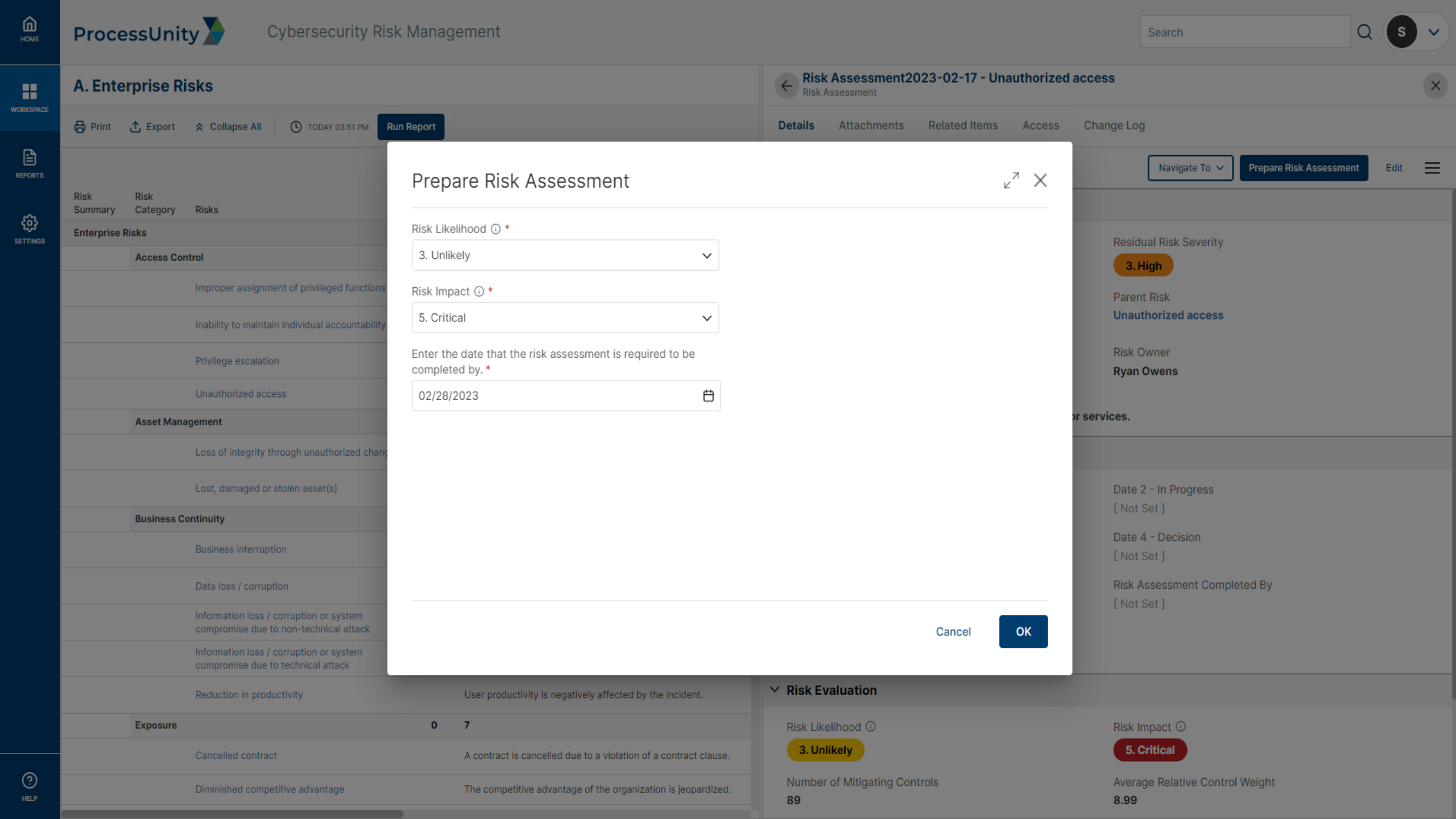
Risk Evaluation

Risk Likelihood
3. Unlikely

Risk Impact
5. Critical

Number of Mitigating Controls
89

Average Relative Control Weight
8.99


ProcessUnity
Cybersecurity Risk Management
Search
HOME
WORKSPACE
REPORTS
SETTINGS
HELP
A. Enterprise Risks
Print
Export
Collapse All
TODAY 03:51 PM
Run Report
Risk Summary
Risk Category
Risks
Enterprise Risks
Access Control
Improper assignment of privileged functions
Inability to maintain individual accountability
Privilege escalation
Unauthorized access
Asset Management
Loss of integrity through unauthorized chang
Lost, damaged or stolen asset(s)
Business Continuity
Business interruption
Data loss / corruption
Information loss / corruption or system compromise due to non-technical attack
Information loss / corruption or system compromise due to technical attack
Reduction in productivity
User productivity is negatively affected by the incident.
Exposure
0
7
Cancelled contract
A contract is cancelled due to a violation of a contract clause.
Diminished competitive advantage
The competitive advantage of the organization is jeopardized.
Risk Assessment2023-02-17 - Unauthorized access
Risk Assessment
Details
Attachments
Related Items
Access
Change Log
Navigate To
Prepare Risk Assessment
Edit
Residual Risk Severity
3. High
Parent Risk
Unauthorized access
Risk Owner
Ryan Owens
or services.
Date 2 - In Progress
[Not Set]
Date 4 - Decision
[Not Set]
Risk Assessment Completed By
[Not Set]
Risk Evaluation
Risk Likelihood
3. Unlikely
Risk Impact
5. Critical
Number of Mitigating Controls
89
Average Relative Control Weight
8.99
Prepare Risk Assessment
Risk Likelihood *
3. Unlikely
Risk Impact *
5. Critical
Enter the date that the risk assessment is required to be completed by. *
02/28/2023
Cancel
OK

A. Enterprise Risks

Print | Export | Collapse All | TODAY 03:51 PM | Run Report

Risk Summary	Risk Category	Risks	Open Plan	Risk Description
Enterprise Risks			**2**	**32**
	Access Control		**1**	**4**
		Improper assignment of privileged functions		There is a failure to implement least privileges.
		Inability to maintain individual accountability		There is non-repu
		Privilege escalation	1	Access t
		Unauthorized access		Access i
	Asset Management		**1**	**2**
		Loss of integrity through unauthorized changes	1	Unautho service.
		Lost, damaged or stolen asset(s)		Asset(s)
	Business Continuity		**0**	**5**
		Business interruption		There is increased latency or a service outage that negatively impa business operations.
		Data loss / corruption		There is a failure to maintain the confidentiality of the data (compr data is corrupted (loss).
		Information loss / corruption or system compromise due to non-technical attack		Social engineering, sabotage or other non-technical attack compro data, systems, applications or services.
		Information loss / corruption or system compromise due to technical attack		Malware, phishing, hacking or other technical attack compromise c systems, applications or services.
		Reduction in productivity		User productivity is negatively affected by the incident.
	Exposure		**0**	**7**
		Cancelled contract		A contract is cancelled due to a violation of a contract clause.
		Diminished competitive advantage		The competitive advantage of the organization is jeopardized.

Risk Assessment2023-02-17 - Unauthorized access

Risk Assessment

Details | Attachments | Related Items | Access | Change Log

Navigate To | Prepare Risk Assessment | Edit

Risk Assessment

Inherent Risk Severity
3. High

Residual Risk Severity
3. High

Assessment Status

Parent Risk
Unauthorized access

Risk Owner
Ryan Owens

d individuals, groups or services.

Date 2 - In Progress
[Not Set]

Date 3 - Due
[Not Set]

Date 4 - Decision
[Not Set]

Date 5 - Complete
[Not Set]

Risk Assessment Completed By
[Not Set]

Risk Assessment Lifecycle in Business Days
[Not Set]

Risk Evaluation

Risk Likelihood
3. Unlikely

Risk Impact
5. Critical

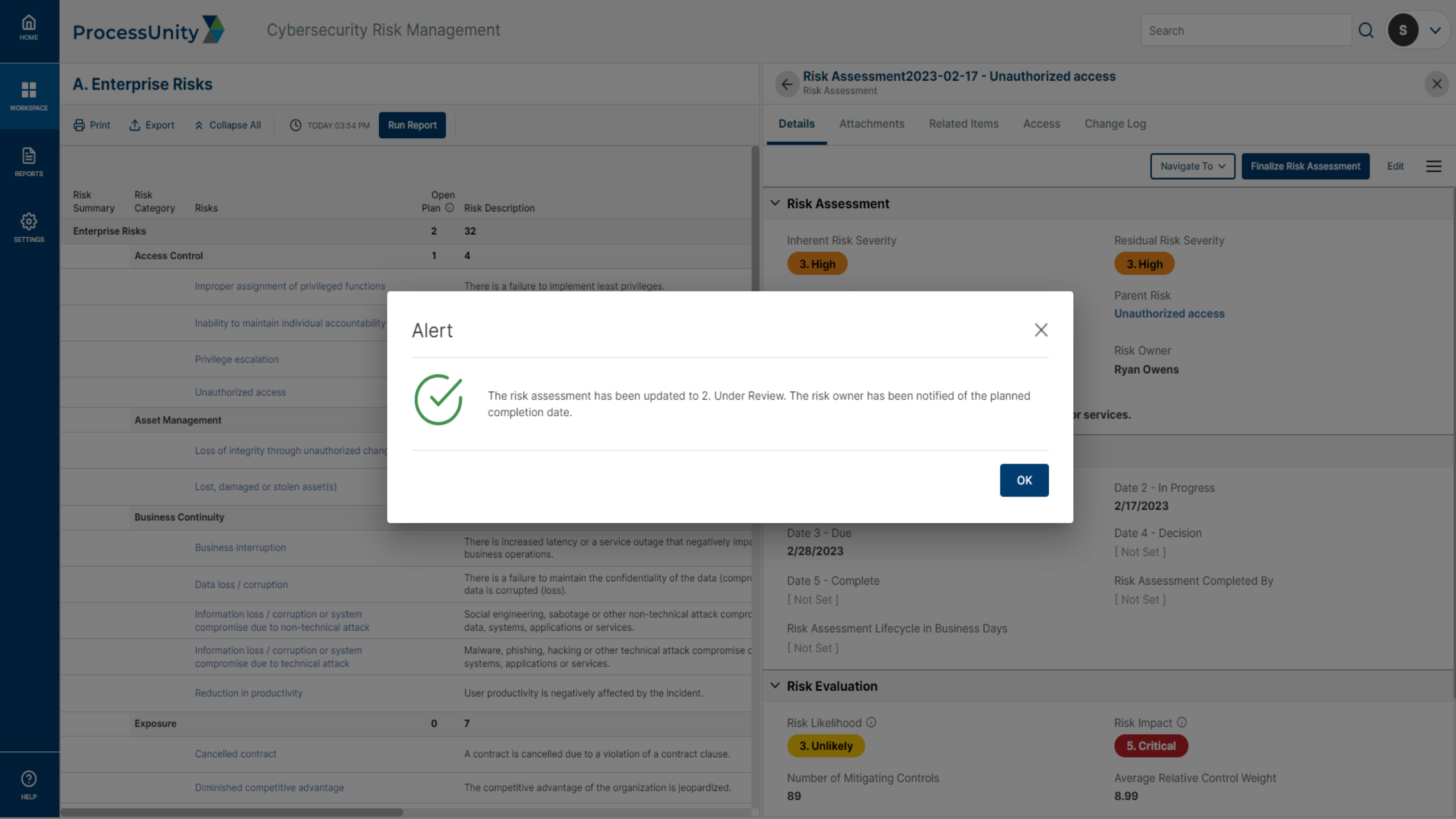
Number of Mitigating Controls
89

Average Relative Control Weight
8.99

Confirm

Are you sure you want to prepare risk assessment? This action will notify the risk owner of the planned completion date.

Cancel | OK


ProcessUnity
Cybersecurity Risk Management
Search
HOME
WORKSPACE
REPORTS
SETTINGS
HELP
A. Enterprise Risks
Print
Export
Collapse All
TODAY 03:54 PM
Run Report
Risk Summary
Risk Category
Risks
Open Plan
Risk Description
Enterprise Risks 2 32
Access Control 1 4
Improper assignment of privileged functions
There is a failure to implement least privileges.
Inability to maintain individual accountability
Privilege escalation
Unauthorized access
Asset Management
Loss of integrity through unauthorized chang
Lost, damaged or stolen asset(s)
Business Continuity
Business interruption
There is increased latency or a service outage that negatively impa business operations.
Data loss / corruption
There is a failure to maintain the confidentiality of the data (compr data is corrupted (loss).
Information loss / corruption or system compromise due to non-technical attack
Social engineering, sabotage or other non-technical attack compro data, systems, applications or services.
Information loss / corruption or system compromise due to technical attack
Malware, phishing, hacking or other technical attack compromise c systems, applications or services.
Reduction in productivity
User productivity is negatively affected by the incident.
Exposure 0 7
Cancelled contract
A contract is cancelled due to a violation of a contract clause.
Diminished competitive advantage
The competitive advantage of the organization is jeopardized.
Risk Assessment2023-02-17 - Unauthorized access
Risk Assessment
Details
Attachments
Related Items
Access
Change Log
Navigate To
Finalize Risk Assessment
Edit
Risk Assessment
Inherent Risk Severity
3. High
Residual Risk Severity
3. High
Parent Risk
Unauthorized access
Risk Owner
Ryan Owens
or services.
Date 2 - In Progress
2/17/2023
Date 3 - Due
2/28/2023
Date 4 - Decision
[Not Set]
Date 5 - Complete
[Not Set]
Risk Assessment Completed By
[Not Set]
Risk Assessment Lifecycle in Business Days
[Not Set]
Risk Evaluation
Risk Likelihood
3. Unlikely
Risk Impact
5. Critical
Number of Mitigating Controls
89
Average Relative Control Weight
8.99
Alert
The risk assessment has been updated to 2. Under Review. The risk owner has been notified of the planned completion date.
OK

A. Enterprise Risks

Print | Export | Collapse All | TODAY 03:54 PM | Run Report

Risk Summary	Risk Category	Risks	Open Plan	Risk Description
Enterprise Risks			**2**	**32**
	Access Control		**1**	**4**
		Improper assignment of privileged functions		There is a failure to implement least privileges.
		Inability to maintain individual accountability		There is a failure to maintain asset ownership and it is not possible non-repudiation of actions or inactions.
		Privilege escalation	1	Access to privileged functions is inadequate or cannot be controlle
		Unauthorized access		Access is granted to unauthorized individuals, groups or services.
	Asset Management		**1**	**2**
		Loss of integrity through unauthorized changes	1	Unauthorized changes corrupt the integrity of the system / applica service.
		Lost, damaged or stolen asset(s)		Asset(s) is/are lost, damaged or stolen.
	Business Continuity		**0**	**5**
		Business interruption		There is increased latency or a service outage that negatively impa business operations.
		Data loss / corruption		There is a failure to maintain the confidentiality of the data (compr data is corrupted (loss).
		Information loss / corruption or system compromise due to non-technical attack		Social engineering, sabotage or other non-technical attack compro data, systems, applications or services.
		Information loss / corruption or system compromise due to technical attack		Malware, phishing, hacking or other technical attack compromise c systems, applications or services.
		Reduction in productivity		User productivity is negatively affected by the incident.
	Exposure		**0**	**7**
		Cancelled contract		A contract is cancelled due to a violation of a contract clause.
		Diminished competitive advantage		The competitive advantage of the organization is jeopardized.

Risk Assessment2023-02-17 - Unauthorized access

Risk Assessment

Details | Attachments | Related Items | Access | Change Log

Navigate To | Finalize Risk Assessment | Edit

Risk Assessment

Inherent Risk Severity
3. High

Residual Risk Severity
3. High

Assessment Status
2. Under Review

Parent Risk
Unauthorized access

Risk Manager
Rachel Miller

Risk Owner
Ryan Owens

Risk Description
Access is granted to unauthorized individuals, groups or services.

Risk Assessment Dates

Date 1 - Open
2/17/2023

Date 2 - In Progress
2/17/2023

Date 3 - Due
2/28/2023

Date 4 - Decision
[Not Set]

Date 5 - Complete
[Not Set]

Risk Assessment Completed By
[Not Set]

Risk Assessment Lifecycle in Business Days
[Not Set]

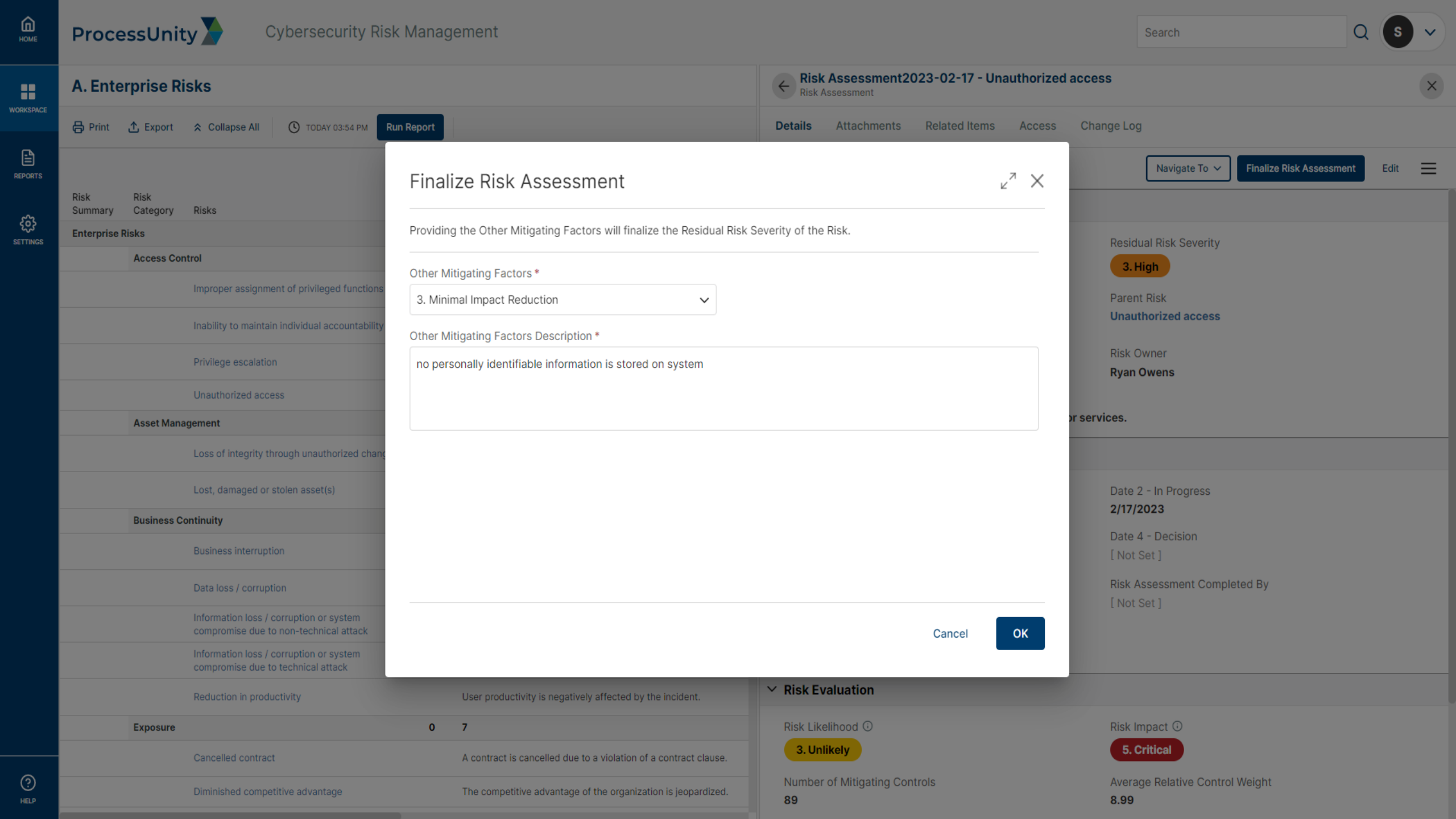
Risk Evaluation

Risk Likelihood
3. Unlikely

Risk Impact
5. Critical

Number of Mitigating Controls
89

Average Relative Control Weight
8.99


ProcessUnity
Cybersecurity Risk Management
Search
HOME
WORKSPACE
REPORTS
SETTINGS
HELP
A. Enterprise Risks
Print
Export
Collapse All
TODAY 03:54 PM
Run Report
Risk Summary
Risk Category
Risks
Enterprise Risks
Access Control
Improper assignment of privileged functions
Inability to maintain individual accountability
Privilege escalation
Unauthorized access
Asset Management
Loss of integrity through unauthorized chang
Lost, damaged or stolen asset(s)
Business Continuity
Business interruption
Data loss / corruption
Information loss / corruption or system compromise due to non-technical attack
Information loss / corruption or system compromise due to technical attack
Reduction in productivity
User productivity is negatively affected by the incident.
Exposure
0
7
Cancelled contract
A contract is cancelled due to a violation of a contract clause.
Diminished competitive advantage
The competitive advantage of the organization is jeopardized.
Risk Assessment2023-02-17 - Unauthorized access
Risk Assessment
Details
Attachments
Related Items
Access
Change Log
Navigate To
Finalize Risk Assessment
Edit
Residual Risk Severity
3. High
Parent Risk
Unauthorized access
Risk Owner
Ryan Owens
or services.
Date 2 - In Progress
2/17/2023
Date 4 - Decision
[Not Set]
Risk Assessment Completed By
[Not Set]
Risk Evaluation
Risk Likelihood
3. Unlikely
Risk Impact
5. Critical
Number of Mitigating Controls
89
Average Relative Control Weight
8.99
Finalize Risk Assessment
Providing the Other Mitigating Factors will finalize the Residual Risk Severity of the Risk.
Other Mitigating Factors *
3. Minimal Impact Reduction
Other Mitigating Factors Description *
no personally identifiable information is stored on system
Cancel
OK

A. Enterprise Risks

Print | Export | Collapse All | TODAY 03:58 PM | Run Report

Risk Summary	Risk Category	Risks	Open Plan	Risk Description
Enterprise Risks			**2**	**32**
	Access Control		**1**	**4**
		Improper assignment of privileged functions		There is a failure to implement least privileges.
		Inability to maintain individual accountability		There is a failure to maintain asset ownership and it is not possible non-repudiation of actions or inactions.
		Privilege escalation	1	Access to privileged functions is inadequate or cannot be controlle
		Unauthorized access		Access is granted to unauthorized individuals, groups or services.
	Asset Management		**1**	**2**
		Loss of integrity through unauthorized changes	1	Unauthorized changes corrupt the integrity of the system / applica service.
		Lost, damaged or stolen asset(s)		Asset(s) is/are lost, damaged or stolen.
	Business Continuity		**0**	**5**
		Business interruption		There is increased latency or a service outage that negatively impa business operations.
		Data loss / corruption		There is a failure to maintain the confidentiality of the data (compr data is corrupted (loss).
		Information loss / corruption or system compromise due to non-technical attack		Social engineering, sabotage or other non-technical attack compro data, systems, applications or services.
		Information loss / corruption or system compromise due to technical attack		Malware, phishing, hacking or other technical attack compromise c systems, applications or services.
		Reduction in productivity		User productivity is negatively affected by the incident.
	Exposure		**0**	**7**
		Cancelled contract		A contract is cancelled due to a violation of a contract clause.
		Diminished competitive advantage		The competitive advantage of the organization is jeopardized.

Risk Assessment2023-02-17 - Unauthorized access

Risk Assessment

Details | Attachments | Related Items | Access | Change Log

Navigate To | Complete Risk Assessment | Edit

Risk Assessment

Inherent Risk Severity
3. High

Residual Risk Severity
3. High

Assessment Status
3. Risk Decision

Parent Risk
Unauthorized access

Risk Manager
Rachel Miller

Risk Owner
Ryan Owens

Risk Description
Access is granted to unauthorized individuals, groups or services.

Risk Assessment Dates

Date 1 - Open
2/17/2023

Date 2 - In Progress
2/17/2023

Date 3 - Due
2/28/2023

Date 4 - Decision
2/17/2023

Date 5 - Complete
[Not Set]

Risk Assessment Completed By
[Not Set]

Risk Assessment Lifecycle in Business Days
[Not Set]

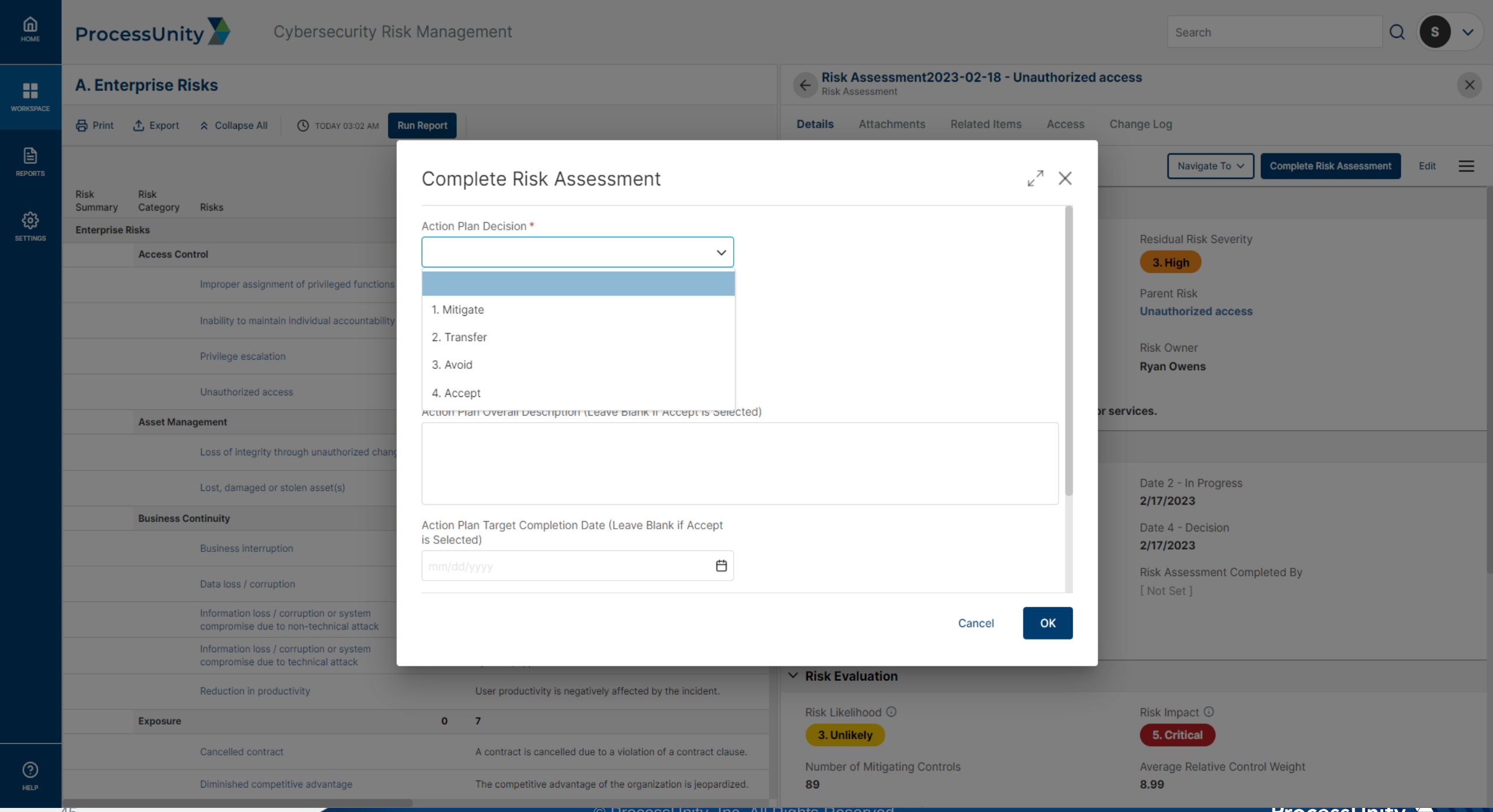
Risk Evaluation

Risk Likelihood
3. Unlikely

Risk Impact
5. Critical

Number of Mitigating Controls
89

Average Relative Control Weight
8.99



A. Enterprise Risks

Print | Export | Collapse All | TODAY 03:59 PM | Run Report

Risk Summary	Risk Category	Risks		
Enterprise Risks				
	Access Control			
		Improper assignment of privileged functions		
		Inability to maintain individual accountability		
		Privilege escalation		
		Unauthorized access		
	Asset Management			
		Loss of integrity through unauthorized chang		
		Lost, damaged or stolen asset(s)		
	Business Continuity			
		Business interruption		
		Data loss / corruption		
		Information loss / corruption or system compromise due to non-technical attack		
		Information loss / corruption or system compromise due to technical attack		
		Reduction in productivity		User productivity is negatively affected by the incident.
	Exposure		0	7
		Cancelled contract		A contract is cancelled due to a violation of a contract clause.
		Diminished competitive advantage		The competitive advantage of the organization is jeopardized.

Risk Assessment2023-02-17 - Unauthorized access

Risk Assessment

Details | Attachments | Related Items | Access | Change Log

Navigate To | Complete Risk Assessment | Edit

Residual Risk Severity
3. High

Parent Risk
Unauthorized access

Risk Owner
Ryan Owens

...or services.

Date 2 - In Progress
2/17/2023

Date 4 - Decision
2/17/2023

Risk Assessment Completed By
[Not Set]

Risk Evaluation

Risk Likelihood
3. Unlikely

Risk Impact
5. Critical

Number of Mitigating Controls
89

Average Relative Control Weight
8.99

Complete Risk Assessment

Action Plan Name (Leave Blank if Accept is Selected)

Unauthorised access

Action Plan Overall Description (Leave Blank if Accept is Selected)

1. Review access roles and responsibilities
2. Review access control policies
3. Implement ACL

Action Plan Target Completion Date (Leave Blank if Accept is Selected)

02/28/2023

Risk Assessment Summary *

Access control has not been fully implemented and needs to be updated ASAP.

Cancel | OK

A. Enterprise Risks

Print | Export | Collapse All | TODAY 03:59 PM | Run Report

Risk Summary	Risk Category	Risks	Open Plan	Risk Description
Enterprise Risks			**2**	**32**
	Access Control		**1**	**4**
		Improper assignment of privileged functions		There is a failure to implement least privileges.
		Inability to maintain individual accountability		There is a failure to maintain non-repudiation of actions
		Privilege escalation	1	Access to privileged funct
		Unauthorized access		Access is granted to unau
	Asset Management		**1**	**2**
		Loss of integrity through unauthorized changes	1	Unauthorized changes co service.
		Lost, damaged or stolen asset(s)		Asset(s) is/are lost, damag
	Business Continuity		**0**	**5**
		Business interruption		There is increased latency or a service outage that negatively impa business operations.
		Data loss / corruption		There is a failure to maintain the confidentiality of the data (compro data is corrupted (loss).
		Information loss / corruption or system compromise due to non-technical attack		Social engineering, sabotage or other non-technical attack compro data, systems, applications or services.
		Information loss / corruption or system compromise due to technical attack		Malware, phishing, hacking or other technical attack compromise c systems, applications or services.
		Reduction in productivity		User productivity is negatively affected by the incident.
	Exposure		**0**	**7**
		Cancelled contract		A contract is cancelled due to a violation of a contract clause.
		Diminished competitive advantage		The competitive advantage of the organization is jeopardized.

Risk Assessment2023-02-17 - Unauthorized access

Risk Assessment

Details | Attachments | Related Items | Access | Change Log

Navigate To | Complete Risk Assessment | Edit

Risk Assessment

Inherent Risk Severity
3. High

Residual Risk Severity
3. High

Assessment Status

Parent Risk
Unauthorized access

Risk Owner
Ryan Owens

to unauthorized individuals, groups or services.

t Dates

Date 2 - In Progress
2/17/2023

Date 3 - Due
2/28/2023

Date 4 - Decision
2/17/2023

Date 5 - Complete
[Not Set]

Risk Assessment Completed By
[Not Set]

Risk Assessment Lifecycle in Business Days
[Not Set]

Risk Evaluation

Risk Likelihood
3. Unlikely

Risk Impact
5. Critical

Number of Mitigating Controls
89

Average Relative Control Weight
8.99

Confirm

Click OK to Continue

Cancel | OK

A. Enterprise Risks

Print | Export | Collapse All | TODAY 04:05 PM | Run Report

Risk Summary	Risk Category	Risks	Open Plan	Risk Description
Enterprise Risks			3	32
	Access Control		2	4
		Improper assignment of privileged functions		There is a failure to implement least privileges.
		Inability to maintain individual accountability		
		Privilege escalation		
		Unauthorized access		
	Asset Management			
		Loss of integrity through unauthorized chang		
		Lost, damaged or stolen asset(s)		
	Business Continuity		0	5
		Business interruption		There is increased latency or a service outage that negatively impa business operations.
		Data loss / corruption		There is a failure to maintain the confidentiality of the data (compr data is corrupted (loss).
		Information loss / corruption or system compromise due to non-technical attack		Social engineering, sabotage or other non-technical attack compro data, systems, applications or services.
		Information loss / corruption or system compromise due to technical attack		Malware, phishing, hacking or other technical attack compromise c systems, applications or services.
		Reduction in productivity		User productivity is negatively affected by the incident.
	Exposure		0	7
		Cancelled contract		A contract is cancelled due to a violation of a contract clause.
		Diminished competitive advantage		The competitive advantage of the organization is jeopardized.

Unauthorized access

Risk

Details | Risk Assessments | Attachments | Related Items | Reports | Access | Change Log

Navigate To | Create Risk Assessment | Edit

Risk

Inherent Risk Severity
3. High

Residual Risk Severity
3. High

Risk Owner
Ryan Owens

Completed Risk Assessments
4

Completed Action Plans
1

or services.

Risk Assessment Frequency
5. Annually

Next Risk Assessment
2/17/2024

Latest Risk Assessment

Last Risk Assessment Sent
2/17/2023

Last Risk Assessment Completed
2/17/2023

Latest Risk Assessment Recommendations
Based off the previous risk assessment's outcome of a high residual risk severity, the program's recommendations are to evaluate the efficiency of existing controls, develop and implement additional control mechanisms, and monitor the risk quarterly.

Risk Likelihood
3. Unlikely

Risk Impact
5. Critical

Number of Mitigating Controls
89

Average Relative Control Weight
8.99

Alert

Risk Assessment Complete and Action Plan has been created. You have been navigated back to the parent Risk.

OK

A. Enterprise Risks

Print | Export | Collapse All | TODAY 04:05 PM | Run Report

Risk Summary	Risk Category	Risks	Open Plan	Risk Description
Enterprise Risks			**3**	**32**
	Access Control		**2**	**4**
		Improper assignment of privileged functions		There is a failure to implement least privileges.
		Inability to maintain individual accountability		There is a failure to maintain asset ownership and it is not possible non-repudiation of actions or inactions.
		Privilege escalation	1	Access to privileged functions is inadequate or cannot be controlle
		Unauthorized access	1	Access is granted to unauthorized individuals, groups or services.
	Asset Management		**1**	**2**
		Loss of integrity through unauthorized changes	1	Unauthorized changes corrupt the integrity of the system / applica service.
		Lost, damaged or stolen asset(s)		Asset(s) is/are lost, damaged or stolen.
	Business Continuity		**0**	**5**
		Business interruption		There is increased latency or a service outage that negatively impa business operations.
		Data loss / corruption		There is a failure to maintain the confidentiality of the data (compr data is corrupted (loss).
		Information loss / corruption or system compromise due to non-technical attack		Social engineering, sabotage or other non-technical attack compro data, systems, applications or services.
		Information loss / corruption or system compromise due to technical attack		Malware, phishing, hacking or other technical attack compromise c systems, applications or services.
		Reduction in productivity		User productivity is negatively affected by the incident.
	Exposure		**0**	**7**
		Cancelled contract		A contract is cancelled due to a violation of a contract clause.
		Diminished competitive advantage		The competitive advantage of the organization is jeopardized.

Unauthorized access

Risk

Details | Risk Assessments | Attachments | Related Items | Reports | Access | Change Log

Navigate To | Create Risk Assessment | Edit

Risk

Inherent Risk Severity
3. High

Residual Risk Severity
3. High

Risk Manager
Rachel Miller

Risk Owner
Ryan Owens

Open Risk Assessments
0

Completed Risk Assessments
4

Open Action Plans
1

Completed Action Plans
1

Risk Description
Access is granted to unauthorized individuals, groups or services.

Risk Scheduler

Risk Assessment Frequency
5. Annually

Next Risk Assessment
2/17/2024

Latest Risk Assessment

Last Risk Assessment Sent
2/17/2023

Last Risk Assessment Completed
2/17/2023

Latest Risk Assessment Recommendations
Based off the previous risk assessment's outcome of a high residual risk severity, the program's recommendations are to evaluate the efficiency of existing controls, develop and implement additional control mechanisms, and monitor the risk quarterly.

Risk Likelihood
3. Unlikely

Risk Impact
5. Critical

Number of Mitigating Controls
89

Average Relative Control Weight
8.99

A. Enterprise Risks

Print | Export | Collapse All | TODAY 04:05 PM | Run Report

Risk Summary	Risk Category	Risks	Open Plan	Risk Description
Enterprise Risks			**3**	**32**
	Access Control		**2**	**4**
		Improper assignment of privileged functions		There is a failure to implement least privileges.
		Inability to maintain individual accountability		There is a failure to maintain asset ownership and it is not possible non-repudiation of actions or inactions.
		Privilege escalation	1	Access to privileged functions is inadequate or cannot be controlle
		Unauthorized access	1	Access is granted to unauthorized individuals, groups or services.
	Asset Management		**1**	**2**
		Loss of integrity through unauthorized changes	1	Unauthorized changes corrupt the integrity of the system / applica service.
		Lost, damaged or stolen asset(s)		Asset(s) is/are lost, damaged or stolen.
	Business Continuity		**0**	**5**
		Business interruption		There is increased latency or a service outage that negatively impa business operations.
		Data loss / corruption		There is a failure to maintain the confidentiality of the data (compr data is corrupted (loss).
		Information loss / corruption or system compromise due to non-technical attack		Social engineering, sabotage or other non-technical attack compro data, systems, applications or services.
		Information loss / corruption or system compromise due to technical attack		Malware, phishing, hacking or other technical attack compromise c systems, applications or services.
		Reduction in productivity		User productivity is negatively affected by the incident.
	Exposure		**0**	**7**
		Cancelled contract		A contract is cancelled due to a violation of a contract clause.
		Diminished competitive advantage		The competitive advantage of the organization is jeopardized.

Unauthorized access

Risk

Details | Risk Assessments | Attachments | Related Items | **Reports** | Access | Change Log

Print | Export | TODAY 04:08 PM | Run Report

View Report

Action Plans

Action Plan State	Action Plan	Action Plan Type	Action Plan Status
1. New	Unauthorised access	1. Mitigate	
C. Completed	Unauthorized access action plan xyz	1. Mitigate	Green

(2 rows)

A. Action Plan Tracker

Show Chart | Print | Export | Reset Report | Collapse All | TODAY 04:15 PM | Run Report

Filters

				Budget / Spend		Action Plan Overview				Personnel		Start Date		Completion Date	
Planned Year	Status	Forecast	Action Plan	Estimated	Actual	Type	Status	Progression	Priority	Originator	Owner	Planned	Actual	Planned	Actual
2023			12	$495,000	$305,500										
	1. New		2	-	-										
		☑	Privilege escalation			Mitigate	New				Charles Ryan			2/23/2023	
		☑	Unauthorised access			Mitigate	New				Charles Ryan			2/28/2023	
	2. Planned		1	$30,000	-										
		☑	Loss of Integrity through unauthorized changes	$30,000		Mitigate	Planned		9	Rachel Miller	Ryan Owens	12/2/2022		3/31/2023	
	C. Completed		8	$450,000	$285,500										
		☑	Privilege Escalation Improvement Plan	$250,000	$50,000	Mitigate	Completed		8		Andrea Walker	1/31/2023	1/16/2023	12/29/2023	1/16/2023
		☑	t Management - Jan-2023	$30,000	$40,000	Mitigate	Completed		9	Matt Bianchi	Andrea Walker	1/20/2023	1/20/2023	1/20/2023	1/20/2023
		☑	Privilege Escalation Priority	$45,000	$50,000	Mitigate	Completed		8		Andrea Walker	1/20/2023	1/20/2023	2/28/2023	1/20/2023
		☑	data loss action plan	$20,000	$25,500	Mitigate	Completed		9		Andrea Walker	1/24/2023	1/23/2023	1/31/2023	1/23/2023
		☑	Unauthorized access action plan xyz	$30,000	$30,000	Mitigate	Completed		9		Andrea Walker	1/24/2023	1/24/2023	1/31/2023	1/24/2023
		☑	Abusive Action Plan	$25,000	$30,000	Mitigate	Completed		8		Andrea Walker	1/31/2023	1/26/2023	1/26/2023	1/26/2023
		☑	Asset Management - Jan-2023	$30,000	$30,000	Mitigate	Completed		7		Andrea Walker	1/31/2023	1/26/2023	2/28/2023	1/26/2023
		☑	Endpoint Security - Dec-2022	$20,000	$30,000	Mitigate	Completed		6	Matt Bianchi	Rachel Miller	1/2/2023	12/2/2022	12/31/2023	2/7/2023
	X. Cancelled		1	$15,000	$20,000										
		☑	diminished competitive advantage	$15,000	$20,000	Mitigate	Cancelled		8		Ryan Owens	11/30/2022	11/30/2022	5/31/2023	11/30/2022
			12	$495,000	$305,500										

Benefits: ProcessUnity Risk Register

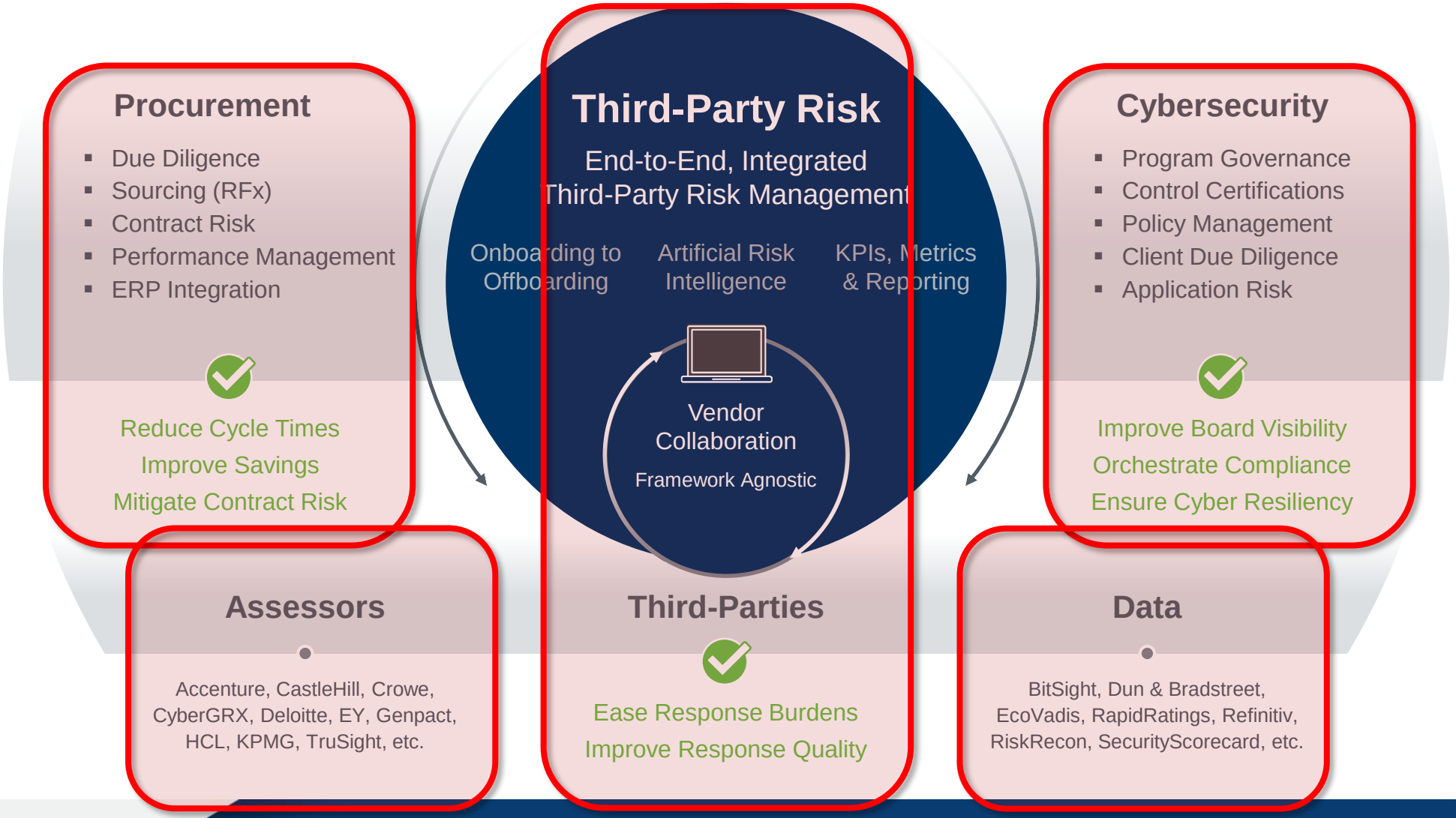
Create a strong foundation for your third-party and cyber risk management

Understand your risk landscape through a heatmap

Develop action plans for vulnerabilities identified in your risk register

The Vision

THE ENTERPRISE THIRD-PARTY + CYBERSECURITY ECOSYSTEM



For More Information

Automate Your Third-Party Risk Management Program:

www.processunity.com/automate

Gartner Report Evaluates Top Vendor Risk Tools:

www.processunity.com/gartner

Contact ProcessUnity:

www.processunity.com/contact

Contact Andrew Egoroff:

andrew.egoroff@processunity.com

SANS

from the most trusted name in information security