Cybersecurity Risk Assessment Procedure

Document ID: **SECSD-01** For: Alliance Federation Approval Date: 2022-02-15 Approved By: NSC

1. Introduction

Cybersecurity risk assessment is a key component of the risk management lifecycle. The purpose of this procedure is to create steps to:

- prepare for risk assessments;
- conduct risk assessments;
- communicate risk assessment results to key organizational personnel;
- maintain the risk assessments over time.

2. Definitions

Refer to SEC-00 Information Security Glossary definitions used in this procedure.

3. Applicability

3.1 This procedure applies to all cybersecurity risks within the scope of *SEC-05 Cybersecurity Risk Management Policy*. National host sites are encouraged, but not obligated to use the same procedure for their cybersecurity risk assessments.

3.2 Roles and responsibilities

Refer to SEC-05 Cybersecurity Risk Management Policy (section 3.2) for the roles and responsibilities associated with risk assessment.

4. Risk Assessment Procedure

4.1 Prepare

4.1.1. Risk categories allow us to group risks into similar areas of reporting. Review Appendix A (Risk categories) prior to starting a risk assessment. Risks must always

be reported under a single category. Please select the category that best matches your risk at the time of assessment.

- 4.1.2. Ensure the scope is well defined, documented, and understood. Review the risk assessment matrix to understand likelihood and impact scoring.
- 4.1.3. Review *SEC-05 Cybersecurity Risk Management Policy* (section 4.3, Responding to risk) to look at treatment approaches

4.2 Identify

- 4.2.1. Identify the asset, service or component that will be assessed. The more granular the assessment the easier it will be to identify distinct or actionable risks. Keep in mind that many services have dependencies, and risks for dependencies should be assessed separately. Refer to the examples provided in the Appendix B for further guidance.
- 4.2.2. Review the threats identified in the risk register and list any that apply directly to the asset, service or component. If you identify a threat that is not already listed on the risk register, it can be proposed to the NSC for consideration as a new threat by email to security@tech.alliancecan.ca. In addition, avoid listing threats against dependencies.
- 4.2.3. Review and ensure awareness of any existing controls that relate to the threats identified in 4.2.2, and summarize. Refer to the examples provided in the Appendix C for further guidance.
- 4.2.4. Following the risk treatment options as indicated in *SEC-05 Cybersecurity Risk Management Policy* (Section 4.3), identify and record the risk treatment plan.
- 4.2.5. Identify mitigating controls in the risk treatment plan and what vulnerabilities are present given the way security control is implemented.
- 4.2.6. Identify the residual likelihood that the threat could compromise the asset/service and the impact to the asset/service.

4.3 Analyze

- 4.3.1. Assess and record in the risk register the inherent likelihood of this risk on a score of 1-5 as defined in the risk matrix, and see Appendix D for examples.
- 4.3.2. Assess and record in the risk register the impact of this risk on a score of 1-5 as defined in the risk matrix, and see Appendix D for examples.
- 4.3.3. Ensure the calculated risk score, based on the likelihood and impact, is recorded in the risk register.

4.4 Evaluate

- 4.4.1. Evaluate the risk based on SEC-05 Cybersecurity Risk Management Policy (section 4.3) and follow the risk management procedures, as required.
- 4.4.2. Taking into account the proposed risk treatment, re-analyze residual risk score.
- 4.4.3. Document treatment and residual risk in the risk register.

4.5 Communicate

- 4.5.1. Once confirmed with the service owner, ensure result(s) are communicated to the NSC with the appropriate level of abstraction, once the assessment programs are complete. Note this will frequently result in multiple risks being communicated at the same time.
- 4.5.2. The risk owner is accountable for communicating information to all impacted stakeholders and sharing risk-related information to the community. Refer to *SEC-05 Cybersecurity Risk Management Policy* (section 4.6) for further details.

4.6 Maintain

- 4.6.1. The risk register should be reviewed on a regular basis. Refer to *SEC-05 Cybersecurity Risk Management Policy* (section 4.5) for further details.
- 4.6.2. It is recommended to schedule a review to ensure ongoing reassessment of risks.

5. References:

SEC-05 Cybersecurity Risk Management Policy

Appendix A: Risk Categories

Each risk category below includes sub categories. Risks are recorded against an individual sub category. Refer to the Risk Register for examples of risks already recorded against sub categories for additional guidance.

Risk Category	Sub Categories	Notes
Human resources and factors	Inadequate support Insufficient skills and knowledge Inadequate resource management Personnel misconduct Social engineering	Includes risks related to human factors such as training, social engineering, and behaviour.
Physical	Theft of physical assets Environmental failure and natural disaster Inadequate datacenter security control	This category includes risks to assets which process, convey, or store information (e.g. servers, thumb drives, network cables, etc.), physical controls (e.g. locks, walls, etc.), and the environments in which these assets & controls reside (e.g buildings, data rooms, conduits, etc.).
System operation	Unmanaged data flow Misconfiguration Resource saturation Documentation error Hardware failure Service unneeded or unauthorized Inability to detect anomalies	Operational issues that create risk, typically related to system resources, their availability and/or correct function and configuration.
Telecommunications	Unauthorised network access Data interception DOS and network congestion	Risks related to networking including denial of service, both malicious or otherwise and unauthorized use of the network.
Software	Malicious software Inadequate software lifecycle Software failure Unauthorised software access	Software related risk, malicious or otherwise - note that misconfiguration of software falls under system operation, this captures bugs and vulnerabilities related to the software itself. Or access to software (IP) that is

		unauthorized.
Access Control and Identity Management	Inadequate repudiation Inadequate access control Inadequate authenticity/identity Abuse of access rights Account compromised	All risks related to identity management, authentication, authorization, and related secrets included insufficient protections.
Data Security and privacy	Inadequate personal information protection Confidentiality breach Integrity breach Availability breach	Risks related to data & information: this is distinct from the technical controls employed to protect it - this captures the risk should one of these breaches occur or lack of adequate practices to prevent them.
Governance	Inadequate ITSM lifecycle management Inadequate accountability Inadequate governance documents	Risks related to governance, typically relating to oversight, policies and procedures or a lack thereof.

Appendix B

Identifying what's in scope

The assessment would look at the configuration of what's in scope for the particular threat, drawing a line between the threat scope and the dependencies that may be realized. With the example of a MFA server VM in Arbutus Cloud.



Example 1: Insufficient authentication controls on the VM vs Insufficient authentication controls on the Data Center Firewall.

- Impact would be isolated to the VM, and its internal dependencies.
- The likelihood of an actor being able to log into the VM and the likelihood of the Firewall are unrelated.

Example 2: Unpatched operating system vs Unpatched Openstack Neutron element.

- Impact would be isolated to the VM and the applications that reside on that system, and its internal dependencies vs the potential impact to all systems in the Openstack environment.
- The likelihood of an actor being able to exploit the vulnerability on the operating system of a VM is unrelated to the ability to exploit the vulnerability in Openstack.

Appendix C

Examples of existing controls that relate to threats

Example 1: Unauthorized network access due to the weak network segmentation.

Example 2: Compromised account due to accidental exposure in clear password, one control would be MFA.

- Identify possible threats related to the risk category and risk sub-category list.
- Talk to the security experts and sysadmins to record the current controls (Current Controls Description in risk register).
- Analyze the current controls as a reference for scoring the likelihood and the impact.

Risk Category	Risk Sub-category	Possible Threats	Current Controls Description
Telecommunications	Unauthorized network access	Malicious users can access network segment beyond their scope	Network segmentation; Perimeter Firewall & Host Firewall
Access Control and Identity Management	Account compromised	Non-Privileged Account is compromised and may be used by malicious users	Require All Remote Login to Use Multi-Factor Authentication

Risk Register:

Appendix D

Examples of using the matrix to achieve risk scores

When calculating the risk score, it is important that everyone adopt a standard approach when considering the likelihood and impact. The following outlines how to approach each score by expanding on the descriptions from the matrix:

Likelihood							
Almost Certain / has occurred	5	5	10	15	20	25	
Likely	4	4	8	12	16	20	
Possible	3	3	6	9	12	15	
Unlikely	2	2	4	6	8	10	
Rare	1	1	2	3	4	5	
		1	2	3	4	5	
		Insignificant	Minor	Moderate	Major	Critical	
		Impact					

Likelihood:

Remember as with the examples in the previous section, existing controls must be taken into account when considering Likelihood.

- Almost Certain (5): Is occurring now or is almost certain to occur within the foreseeable future.
 - Meaning that this risk is known to be occurring currently in other locations. A good example of this might be an exploit that is currently being used by bad actors in the wild at other similar organizations or on other similar infrastructure.
- Likely (4): Likely to occur within the foreseeable future (is known to have occurred at other similar institutions with similar configurations and/or controls)
 - In this case, there is awareness that this has occurred at other similar organizations or on their infrastructure but there is no indication it is happening right at this moment. Similar to the example above, this may relate to a

vulnerability that has been exploited in similar environments but there is no evidence of current exploitation.

- **Possible (3)**: May occur within the foreseeable future (is known to have occurred elsewhere)
 - This score relates to risks that have occurred infrequently in other different environments, in a different industry, country, or with different conditions. There is no evidence it has occurred in similar circumstances, though.
- Unlikely (2): Not likely to occur within the foreseeable future but is still possible
 - There is no evidence this has ever occurred; however, it doesn't require the same exceptional circumstances to occur (compared to score 1), so it can be set apart from score 3 by lack of evidence and score 1 because exceptional circumstances are not required for it to occur.
- **Rare (1):** Unlikely to occur except in exceptional circumstances
 - This score refers to risk that is almost theoretical in nature. Examples include floods in an area that has never flooded, meteor impacts, civil unrest causing damage to a data centre etc...

Impact:

When considering Impact, there are many factors that can be taken into account (see the table below) When thinking about Impact, assume what would happen if the risk occurs. Then estimate the impact. Look through all the possible factors and find the one that has the highest score. That is the score that should be used when calculating the risk score. Even if all the other factors may be insignificant if even one was critical then the score would be critical.

Sharing allow: TLP - GREEN

Approved

No effect for sites' ability to provide all services to all users sites can still provide all critical services to all users Impacted sites provide all critical ability to provide ability to provide ability to provide all critical services to all users All sites have lost the ability to provide a critical service to a subset of system users All sites are no longer able to provide some critical services any users Functional users users users but has lost efficiency critical service to a subset of system All sites have lost the ability to provide a critical service to a subset of system users All sites are no longer able to provide some critical services No information is exfiltrated, changed, deleted, compromised Low risk information is exfiltrated, changed, deleted, compromised Medium Risk exfiltrated, changed, deleted, compromised High or Very-High risk information is suspected to be exfiltrated, compromised High or Very-High risk information is compromised High or Very-High risk is confirmed to be exfiltrated, compromised		Critical	Major	Moderate	Minor		Factors
Functional ability to provide all services to all users provide all critical services to all users have lost the services to all users but has lost efficiency provide all critical services to all users but has lost efficiency provide all critical services to ability to provide a subset of system users provide some critical services to any users No information is exfiltrated, changed, deleted, compromised Low risk information is exfiltrated, changed, deleted, compromised Medium Risk information is exfiltrated, compromised High or Very-High risk information is suspected to be exfiltrated, changed, deleted, or otherwise High or Very-High risk information is compromised	er able to	All sites are no longer a	All sites have lost the ability to	Impacted sites	sites can still	No effect for sites'	140000
Functional all services to all users services to all services to all users but has lost efficiency ability to provide a subset of system users subset of system users any users Functional users users but has lost efficiency critical service to a subset of system users or a national service is national service is No information is exfiltrated, changed, deleted, compromised Low risk Medium Risk information is information is exfiltrated, changed, deleted, High or Very-High risk information is suspected to be exfiltrated, changed, deleted, or otherwise compromised High or Very-High risk information is compromised Information exfiltrated, compromised exfiltrated, changed, deleted, or otherwise exfiltrated, changed, deleted, or otherwise compromised compromised compromised compromised compromised compromised	ervices to	provide some critical ser	provide a critical service to a	have lost the	provide all critical	ability to provide	
Functional users users but has lost critical service to a efficiency subset of system users or a national service is No information is Low risk Medium Risk High or Very-High risk information exfiltrated, information is information is is suspected to be exfiltrated, is confirmed to be suspected to be changed, deleted, confirmed to be suspected to be changed, deleted, or otherwise or otherwise exfiltrated, exfiltrated, compromised compromised. compromised changed, deleted, changed, deleted, or or compromised changed, deleted, changed, deleted, compromised. compromised compromised compromised compromised.		any users	subset of system users	ability to provide a	services to all	all services to all	
Information Inform				critical service to a	users but has lost	users	Functional
users or a national service is No information is Low risk Medium Risk High or Very-High risk information High or Very-High risk informatio exfiltrated, information is information is is suspected to be exfiltrated, is confirmed to be exfiltrated changed, deleted, confirmed to be suspected to be changed, deleted, or otherwise or otherwise exfiltrated, exfiltrated, compromised compromised. compromised changed, deleted, changed, deleted, OR or otherwise or otherwise Medium Risk information is compromised compromised compromised compromised compromised.				subset of system	efficiency		
Information Inform				users or a			
No information is Low risk Medium Risk High or Very-High risk information High or Very-High risk information exfiltrated, information is information is information is is suspected to be exfiltrated, is confirmed to be exfiltrated, changed, deleted, confirmed to be suspected to be changed, deleted, or otherwise changed, deleted, or otherwise or otherwise exfiltrated, exfiltrated, compromised compromised. compromised changed, deleted, or otherwise or otherwise or otherwise compromised. or otherwise or otherwise or otherwise or otherwise or otherwise compromised.				national service is			
Information exfiltrated, changed, deleted, or otherwise information is compromised information is compromised is suspected to be suspected to be changed, deleted, or otherwise is confirmed to be exfiltrated, changed, deleted, or otherwise Information or otherwise compromised exfiltrated, changed, deleted, changed, deleted, compromised exfiltrated, changed, deleted, changed, deleted, compromised or compromised or compromised	nformation	High or Very-High risk info	High or Very-High risk information	Medium Risk	Low risk	No information is	
Information changed, deleted, confirmed to be suspected to be changed, deleted, or otherwise changed, deleted, or otherwise compromised compromised changed, deleted, changed, deleted, compromised compromised.	filtrated,	is confirmed to be exfilt	is suspected to be exfiltrated,	information is	information is	exfiltrated,	
Information or otherwise exfiltrated, exfiltrated, compromised compromised. compromised changed, deleted, changed, deleted, OR or otherwise or otherwise Medium Risk information is compromised compromised compromised to be exfiltrated.	otherwise	changed, deleted, or oth	changed, deleted, or otherwise	suspected to be	confirmed to be	changed, deleted,	
compromised changed, deleted, changed, deleted, OR or otherwise or otherwise Medium Risk information is compromised compromised confirmed to be extiltrated	L	compromised.	compromised	exfiltrated,	exfiltrated,	or otherwise	Information
or otherwise or otherwise Medium Risk information is			OR	changed, deleted,	changed, deleted,	compromised	monidation
compromised compromised confirmed to be evfiltrated			Medium Risk information is	or otherwise	or otherwise		
compromised compromised commented to be exitinated,			confirmed to be exfiltrated,	compromised	compromised		
changed, deleted, or otherwise			changed, deleted, or otherwise				
Single non- Single non- Single privileged Privileged user account was A privileged user account was	ount was	A privileged user accourt	Privileged user account was	Single privileged	Single non-	Single non-	
privileged user privileged user user account is compromised and has been used compromised and is actively	actively	compromised and is ac	compromised and has been used	user account is	privileged user	privileged user	
account is account was suspected to have in the past by an un-authorized being used by an un-authorize	uthorized	being used by an un-aut	in the past by an un-authorized	suspected to have	account was	account is	
suspected to have compromised been user user and/or		user and/or	user	been	compromised	suspected to have	
Compromised been compromised OR More than one privileged use	ged user	More than one privilege	OR	compromised		been	Compromised
Accounts compromised or A significant number of user accounts have been compromised	npromised	accounts have been comp	A significant number of user	or		compromised	Accounts
More than a single accounts have been compromised or suspected to have been	e been	or suspected to have t	accounts have been compromised	More than a single			
user account was compromised	1	compromised		user account was			
composited to				compromised or susported to			
or suspected to	lent is not	Recovery from the incider	Time to recovery is uppredictable.	Time to recovery is	Time to recovery is	Time to recovery is	
mile to recovery is time to recovery is time to recovery is appendicable recovery non-the inclusion and the second state of th	ive data	nossible (e.g. sensitive	with outside beins	unpredictable	predictable with	predictable with	
Recoverabilit cite evicting internal resources with internal evictime response (c.e., sensitive unit	nublicly).	exfiltrated and posted p	with outside helps	with internal	internal resources	site existing	Recoverabilit
y resources resources outside launch investigation	tion	launch investigatic		resources: outside	memarresources	resources	у
helps are not		iddifen intestigatio		helps are not		resources	
No impact Minor staff Minor iob losses. Risk of death or injury related Actual or high risk of death o	death or	Actual or high risk of de	Risk of death or injury related	Minor iob losses.	Minor staff	No impact	
Productivity disruption. or or significant loss higher than insignificant. or major injury		iniury	higher than insignificant, or major	or significant loss	disruption, or		Productivity
& Human minor loss of of productivity (> job losses			job losses	of productivity (>	minor loss of		& Human Exotors
productivity (<30 or = 30 person			-	or = 30 person	productivity (<30		Tactors
Insignificant Some loss of Some loss Significant loss of confidence for Significant loss of confidence	fidence in	Significant loss of confid	Significant loss of confidence for	Some loss	Some loss of	Insignificant	
impact to user confidence for confidence for impacted site(s) the Alliance Federation; nam	on; name	the Alliance Federation	impacted site(s)	confidence for	confidence for	impact to user	D
experience/public impacted services impacted site(s) becomes a byword for	d for	becomes a byword f		impacted site(s)	impacted services	experience/public	neputation
perception only organizational misconduct or	nduct or	organizational miscond			only	perception	
No regulator Regulator requires Regulator issues Regulator issues notice to comply One or more site shut down, c	down, or	One or more site shut do	Regulator issues notice to comply	Regulator issues	Regulator requires	No regulator	
Regulatory interest; report to regular reporting an enforceable under penalty of service executives face personal lega	nal legal	executives face persona	under penalty of service	an enforceable	regular reporting	interest; report to	Regulatory
regulator is until resolution undertaking termination liability		liability	termination	undertaking	until resolution	regulator is	

Example 1: Unauthorized network access due to the weak network segmentation.

In this example there is evidence that Unauthorized network access has occurred in other similar organizations. There is no evidence of current exploitation however. Also taking into account the current controls such as Network segmentation; Perimeter Firewall & Host Firewall there is no evidence of this occurring in a similar environment but it is certainly possible. This results in a likelihood score of 3.

Looking at impacts if this risk occurred is less straightforward and different people may assess different factors somewhat differently, however, when considering impacts the highest score that seems reasonable for this risk is Moderate (3).

Using the matrix with an Impact of 3 and a Likelihood of 3 the risk score is 9.

Example 2: Non-Privileged Account is compromised and may be used by malicious users.

In this example we have evidence that this has occurred within our own infrastructure. There is no evidence it is currently happening. Given the current controls there is a good chance it will happen again and the likelihood score is assessed at Likely (4).

For impact it is important to note this is a non-privileged account, when considering all the impact factors it is assessed at between Minor (2) and Moderate (3).

Using the matrix with an Impact of 3 and a Likelihood of 4 the risk score is 12.

Simulated Risk Register example:

Risk Category	Risk Sub-category	Possible Threats	Current Controls Description	Threat Likelihood (1-5)	Impact (1-5)	Risk Score (Likelihood × Impact) (1-25)
Telecommuni cations	Unauthorised network access	Malicious users can access network segment beyond their scope	Network segmentation; Perimeter Firewall & Host Firewall	3	3	9
Access Control and Identity Management	Account compromised	Non-Privileged Account is compromised and may be used by malicious users	Require All Remote Login to Use Multi-Factor Authentication	4	3	12