Sharing allow:
TLP - GREEN

Approved

Cybersecurity Risk Management Policy

Document ID: **SEC-05**
For: Alliance Federation
Approval Date: 2022-02-15
Approved By: CSAC

1. Introduction

Cybersecurity risk is a subset of organizational risk, which relates to the confidentiality, integrity and availability of the implementation, operation and management of information systems. It represents an important component which must be addressed as part of ongoing risk management responsibilities.

The purpose of this policy is to:

- Promote a culture of risk-based cybersecurity management across the Alliance Federation;
- Establish appropriate governance structures for managing risks;
- Help individuals within the Alliance Federation understand their responsibilities for cybersecurity risks associated with systems;
- Ensure the lifecycle of the Alliance Federation cybersecurity risk management process is effectively conducted across the organization.

2. Definitions

Refer to *SEC-00 Information Security Glossary* definitions used in this Policy.
In the event of a discrepancy between the definitions below and those in the Glossary, the definitions in the Glossary take precedence.

- **Risk**: Risk is an uncertain event or condition which, if it occurs, affects the ability of an organization to achieve its operational or strategic objectives.
- **Risk Management:** The planned and systematic approach for the identification, assessment, response and monitoring of risk to maximize opportunities and minimize losses.
- **Risk Tolerance:** Risk tolerance is how much risk an organization can withstand to achieve its strategic objectives.
- **Risk Owner:** the role primarily responsible for the effective management of a specific risk or risk category. This is typically an executive or management role that has the

authority and accountability to assume risk on behalf of the organization and ensure risks are effectively managed.

- **Service Owner:** the role primarily accountable for the effective management (including the action required to respond, document, and monitor risks as directed by the Risk Owner) of a specific service, infrastructure, or service portfolio.
- **Accountable:** the role ultimately answerable for the activity or decision
- **Responsible:** the role(s) that has an obligation and is authorized to perform the task. This can be shared between multiple roles.
- **National Service:** Advanced Research Computing (ARC) and related capabilities offered by the Alliance Federation (see service map)

3. Applicability

3.1 This policy applies to the cybersecurity risks associated with the people, processes and technology required to implement, operate and manage national services. Elements that have no dependencies with national services are considered out of scope.

3.2 Roles and responsibilities (RACI matrix)
The following table outlines the Responsibility, Accountability, Consulted, and Informed parties including Cybersecurity Advisory Council (CSAC), National Security Council (NSC), Risk Owners, Service Owners, and Alliance Federation Communications:

	CSAC	**NSC**	**Risk owner**	**Service owner**	**Comms**
Risk register		A	R	R	
Communicating risk	I	C	A	C	R
Assessing risk		I	R	A	
Responding to risk	I	I	A	R	
Accepting risk	I	I	A	R	
Monitoring risk	I	R	C	A	

A = Accountable, R = Responsible, C = Consulted, I = Informed

For a given identified risk, the service owner and risk owner need to be identified and need to be reviewed with the appropriate governance bodies.

4. Apply Risk Management Policy

4.1 Ownership

For each National Service, a Service Owner and Risk Owner must be identified and recorded in the Risk Register. In the situation where identification of ownership is not possible, CSAC in conjunction with the Digital Research Alliance of Canada will assist in establishing the roles.

4.2 Assessing Risk

Risks in scope of this policy must be assessed by following the Alliance Federation risk assessment procedure using the Alliance Federation risk assessment matrix and recorded in the *Alliance Federation Risk Register*. Refer to the risk matrix section 5.

4.3 Treating Risk

Where feasible, all risks should be treated. If the risk score is 8 or above based on the risk assessment procedure, it must be treated as directed by the NSC in a timely manner. Before considering accepting a risk, the risk should be reduced to the smallest possible residual risk using one or more risk treatment approaches. These include but are not limited to:

- Mitigation / Reduction: Implementing controls to reduce the likelihood or consequence of risk
- Avoidance: Deciding not to proceed with the architectures or activity that introduced the unacceptable risk, or choosing an alternative that does not involve the risk.
- Transference / Sharing: Involving a 3rd party (eg: Insurance) to shift the impact of the risk

4.4 Accepting Risk

Acceptance of residual risk score above 8 must be approved by Service Owner in consultation with CSAC and must follow the risk acceptance procedure in the risk management procedures and documented.

4.5 Monitoring Risks

The risk register should be reviewed regularly and at a minimum once a year. The review must include a re-assessment of risks based on identified changes to organizational information systems and the environments in which the systems operate that may affect risk (change monitoring) including changes in the feasibility of the ongoing implementation of risk response measures. Risks that have been accepted should be re-evaluated at every cycle. Efforts should be made to optimize risk response measures, where feasible.

4.6 Communicating & Reporting Risks

Any updates to the risk register should be communicated so that appropriate Alliance Federation stakeholders are made aware of risks and their treatment. Significant changes should be reported to CSAC.

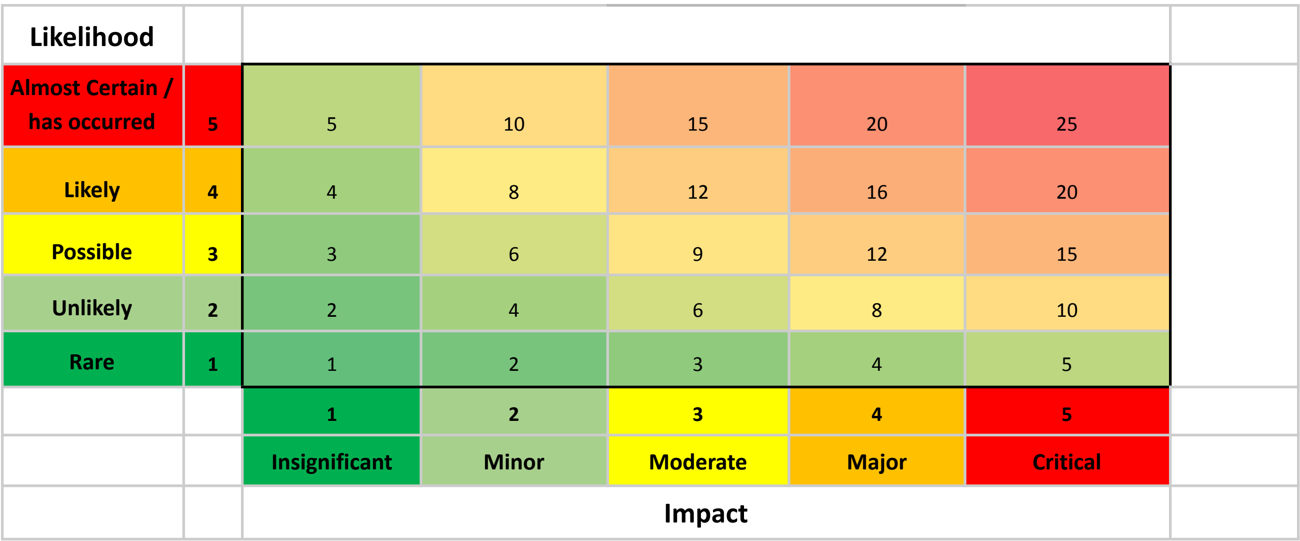
5. Related Information

SEC-00 Information Security Glossary

Risk Assessment Procedure

Alliance Federation Risk Register

Risk 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					