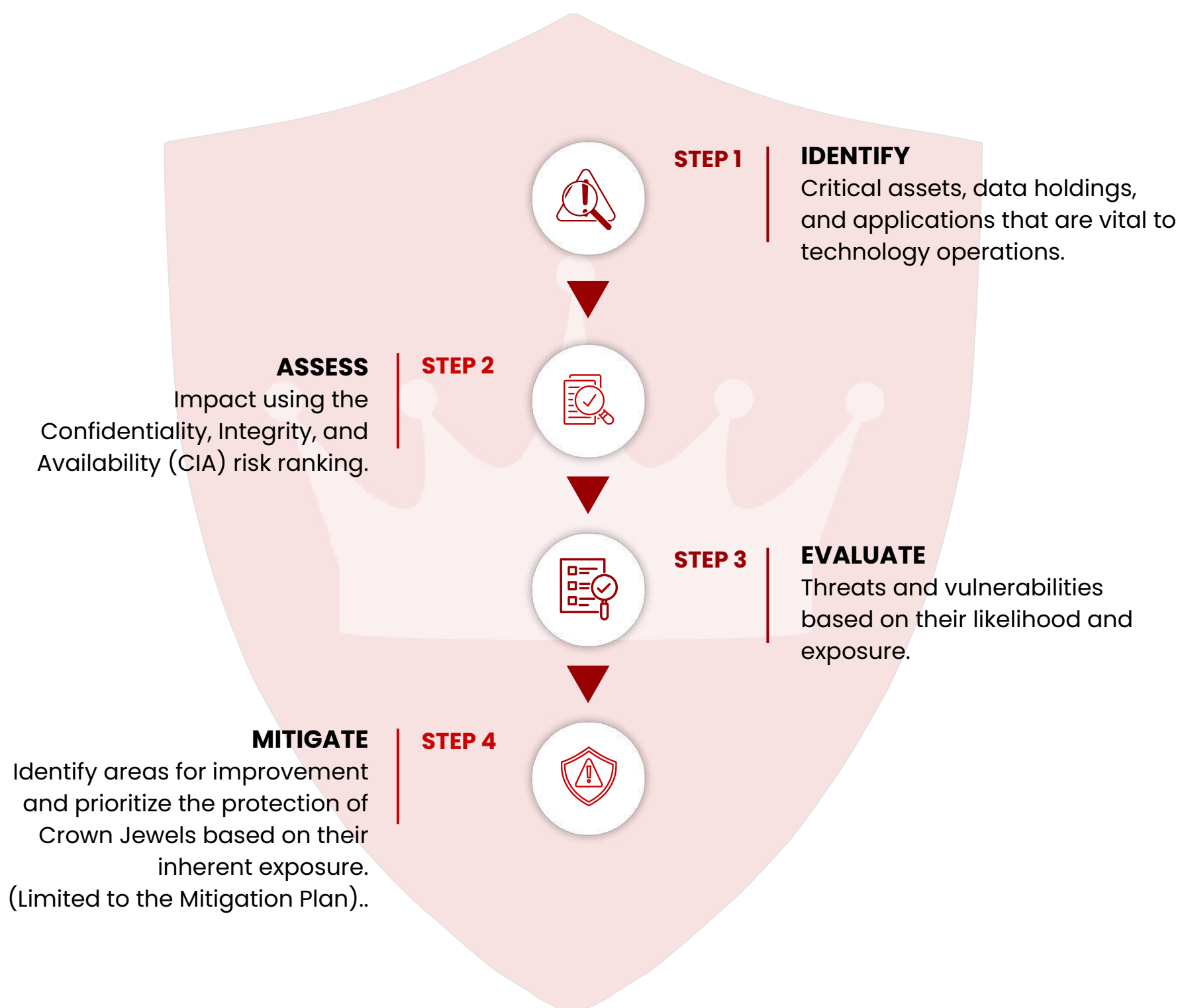# ARANCIA

Crown Jewels Assessment

The threat landscape has evolved, and AI-powered adversaries are executing double extortion attack scenarios targeting sensitive, private data. Identifying and securing an organization's most critical information assets—its Crown Jewels—is essential for resilience against these malicious threat actors.

Mission-critical information assets — an organization's Crown Jewels—are the assets of greatest value and would cause significant business impact if compromised. Too often, organizations recognize the value of these assets but fail to recognize the extent to which they are exposed to threats.

Arancia's Crown Jewels Assessment (CJA) is a foundational exercise that provides a structured approach to identifying, assessing, and safeguarding an organization's most valuable digital and physical assets, improving business continuity, regulatory compliance, and cyber risk mitigation.

Protecting the Crown Jewels
Arancia's CJA follows a structured four-phase methodology:

STEP 1

IDENTIFY
Critical assets, data holdings, and applications that are vital to technology operations.

ASSESS
Impact using the Confidentiality, Integrity, and Availability (CIA) risk ranking.

STEP 2

STEP 3

EVALUATE
Threats and vulnerabilities based on their likelihood and exposure.

MITIGATE
Identify areas for improvement and prioritize the protection of Crown Jewels based on their inherent exposure.
(Limited to the Mitigation Plan)..

STEP 4

Methodology & Process

Arancia's CJA follows a four-step methodology, aligning with industry best practices and frameworks:

STEP 1 — **IDENTIFY ASSETS**
- Define and identify what constitutes a mission-critical information asset.
- Conduct internal workshops and interviews to document mission-critical information assets.
- Categorize assets by function: Applications, Databases, Devices, Network Infrastructure, and Business Systems.

STEP 2 — **ASSESS IMPACT**
- Apply CIA risk rankings to evaluate potential threats, including data breaches, system failures, and operational disruptions.
- Assess the business impact on revenue, reputation, regulatory compliance, and service continuity.

STEP 3 — **IDENTIFY THREATS & VULNERABILITIES**
- Perform a threat and vulnerability analysis to identify internal and external threats.
- Identify threat events likely to target mission-critical information assets.
- Evaluate the level of exposure for each mission-critical information asset.
- Classify vulnerabilities, including misconfigurations, outdated software, unauthorized access risks, and data leaks.
- Map assets to potential attack vectors such as phishing, ransomware, DDoS, and supply chain attacks.

STEP 4 — **PRIORITIZE & REPORT**
- Assign inherent exposure rankings to prioritize mitigation efforts.
- Develop an actionable cybersecurity enhancement roadmap aligned with business objectives.
- Present executive risk dashboard with insights for leadership decision-making.

Key Areas Covered

01 Asset Inventory
Cataloging critical digital and physical assets.

02 Risk Impact Analysis
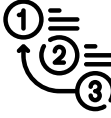Evaluating business, financial, operational, and compliance risks.

03 Threat Modelling
Identifying and assessing key potential attack vectors, threat events, including insider threats and external adversaries.

04 Vulnerability Prioritization
Evaluate the level of exposure to each mission-critical information asset and prioritize based on business impact.

05 Compliance Assurance
Aligning with legal and regulatory frameworks (PIPEDA, ISO 27001, NIST, GDPR, PHIPA, FIPPA).

ARANCIA

Assessment Deliverables

Upon completion, Arancia's CJA provides:

Crown Jewels Inventory Report

A structured list of critical assets, categorized by risk level.

Impact Assessment & Threat Exposure Analysis

A comprehensive risk evaluation using the CIA model.

Inherent Exposure Dashboard

A visual representation of prioritized risks and mitigation efforts.

Remediation Roadmap

A phased action plan for securing critical assets and addressing vulnerabilities.

Threat and Vulnerability Mapping

A ranking system for inherent threats and weaknesses.

Why Arancia?

Over 2 decades of **expertise** and a commitment to **excellence.**

Industry-compliant methodologies (NIST, ISO 27001, Zero Trust, MITRE ATT&CK).

Expert-led assessments tailored for organizations with complex IT infrastructures.

Actionable insights enabling **proactive security enhancements** and business resilience.

Protect Your Crown Jewels with Arancia

Your organization's most valuable assets deserve the highest level of protection. Arancia's Crown Jewels Assessment empowers you with the insights and strategies needed to safeguard mission-critical information, mitigate cyber risks, and ensure compliance.

Don't wait for a breach—take a proactive approach to securing your business-critical assets today.

Contact Arancia at inquiry@arancia.ca