AGILE RISK ASSESSMENT FRAMEWORK (ARAF)

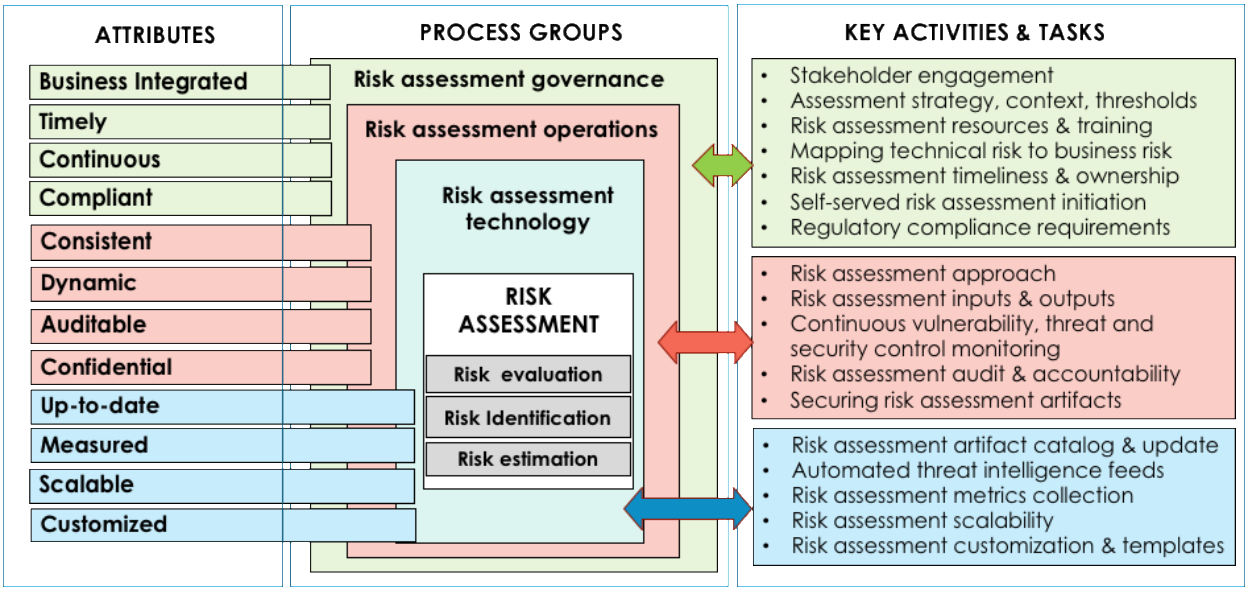
1. Introduction

Identifying and managing cyber risk, one of the most worrisome areas of Enterprise Risk Management (ERM), is critical for any organization's sustainability. As a valuable contributor to achieving business objectives, many organizations leverage risk assessments, as part of ERM activities, to identify, analyze, and evaluate cyber risk. However, traditional risk assessments are lately perceived as a hindrance to business enablement due to their inability to support digital transformations. Some of the drawbacks of the traditional risk assessments include but not limited to:

- Inability to match the fast pace of agile and DevOps methodologies due to lengthy risk assessment completion timeliness – Traditional risk assessments usually take four to six weeks to complete depending on the complexity of the internal and external context. Agile and DevOps initiatives focus on providing rapid and frequent deliveries, usually two to four weeks to release a new feature. As such, traditional risk assessment activities cannot match the pace of agile and DevOps and become easily a bottleneck.
- Incapable risk identification for the emerging technologies such as cloud, IoT, microservices, containers, and APIs by using outdated one-size-fit-all risk assessment templates - Trying to overlay business agility with traditional "one-size-fits-all" point-in-time risk assessments are not scalable. Risk assessments should be customizable to effectively identify the risks in both existing and new technologies and methodologies.
- Inconsistent and subjective risk findings, ratings, and remediation advice due to variations in risk assessment expertise – Risk assessments can be inconsistent and subjective across team members depending on their risk assessment experience and how well they know internal and external policy, standards, requirements, and processes. Inconsistent risk findings, ratings and advise might result in friction between business and risk teams.
- Inadequate risk assessment coverage of new initiatives due to global resource shortage in risk and cybersecurity domains – Risk assessments should be made scalable to capture and manage risk, even in the face of rapidly increasing number of initiatives or insufficient risk assessment resources.
- Inability to include emerging threat, vulnerability and ever-changing regulatory requirements into existing risk assessments due to their static nature – Threat and vulnerability landscapes are rapidly changing. Regulatory requirements evolve rapidly as well. To manage the cyber risk in these dynamic environments require
- Insufficient stakeholder engagement and transparency in risk assessment activities due to siloed risk management approach – Without the full participation of relevant stakeholders, especially from business side, risk assessments will be based on guesswork. Risk assessment approach should allow stakeholders a transparent visibility in the activities to eliminate waste and enhance agility.

Simply, the traditional risk assessment methodologies are not able to enable business units in a timely manner. Risk assessment activities need to be more agile to better manage cyber risk in order to support ever increasing digital transformation initiatives in a timely, consistent, and

traceable manner. Thus, a risk assessment framework is needed with an approach for categorizing and assessing cyber risks dynamically and rapidly. The ARAF, Agile Risk Assessment Framework, has been developed to allow organizations to achieve sustainable progress in risk assessments while maintaining both speed in execution and a strong risk culture. The ARAF changes the traditional focus of risk assessments as a static, procedural activity to a more dynamic approach that provides the capability to effectively manage cyber risks in highly diverse environments. It contains processes, attributes, activities, and tasks that are to be applied during the cyber risk assessments and risk communication.



2. Purpose and applicability

The purpose of the ARAF is to provide guidance to organizations on the design, implementation, operation, and maintenance of continuous and agile cyber risk assessment practices.

Thanks to its flexibility to fit in any ERM model, the ARAF is applicable to all organizations performing risk assessments or considering to implement agile risk assessment practices. Since the ARAF is not industry or sector specific, the application of the agile risk assessment guidelines can be customized to any organization and its internal and external context.
It is recognized that particular projects or organizations may not need to use all of the processes provided by this framework. Therefore, implementation of this framework typically involves selecting a set of attributes and associated activities suitable to the organization or project.

3. Attributes of ARAF

The ARAF has the following attributes to achieve continuous, dynamic and agile risk assessments by executing defined key results:

- business integrated – business stakeholders are transparently and actively involved in risk assessment activities with well-defined accountability and responsibilities
- timely – risk assessments are delivered to the stakeholders within the appropriate time period.
- consistent – the way in which risk assessments are conducted should be well structured to provide consistency throughout an organization
- customized – risk assessments are customized to address risk proportional to asset criticality, internal and external policies, technology selection, financial impact, legal and regulatory mandate.
- dynamic - risk assessments should be responsive to change, emerging threats, and vulnerabilities
- continuous – risk assessment service should be offered continuously
- auditable – The actions of all parties having authorized access to risk assessment activities should be recorded so that this history can be reviewed and used for accountability purposes.
- up-to-date (current) – risk information and guidance provided to stakeholders should be current and kept up to date.
- measured – risk assessments should produce risk metrics that can be used to evaluate effectiveness of existing controls, facilitate comparability of risk results and benchmarking
- confidential – The confidentiality of the risk assessment should be protected.
- compliant – satisfies internal and external compliance requirements
- scalable – The risk assessment activities should be scalable to the size of stakeholder community.

4. Implementation of ARAF

The ARAF groups the cyber risk assessments activities into three process groups:

- Governance process group
- Operational process group
- Technology process group

Each of the processes within those groups satisfies the risk assessment attributes and is described in terms of its purpose, desired outcomes, lists of activities and tasks which need to be performed to achieve the desired outcomes.

The practices described are not exhaustive but provide a baseline for implementation of the ARAF. They can be tailored and responsive to the organization's external and internal context including its mandate, priorities, organizational risk culture, risk management capacity, and partner and stakeholder interests.

It is the responsibility of each organization, individually, to identify the specific actions required to implement the principles and guidance, giving due consideration to the nature of the organization, and appropriate analysis of the risks and opportunities. As a basis for illustration, the practices described are applicable to most organizations (large or small), most of the time.

4.1 Governance Process Group

The organization shall implement the following activities and tasks in accordance with applicable organization policies and procedures with respect to the business governance processes.

4.1.1 Business integration process and activities

Objective: Provide business stakeholders an end-to-end access to risk assessment activities in a cross-functional collaboration team environment.

Key Results:

- Business engagement and participation in risk assessment process are improved
- A self-served risk assessment process and procedures are developed to facilitate business engagement
- Roles and responsibilities as well as accountable risk owners are defined
- Training and awareness sessions to all risk stakeholders are provided
- Appropriate and timely involvement of stakeholders are encouraged
- Usage of business impact and business risk terms in risk assessments are increased
- Technical risk is translated to business risk in risk assessment reports

Activities and Tasks:

- **Involve relevant stakeholders in the decision-making.**
  This activity leverages agile oriented collaborative communication to draw on experience and knowledge from various stakeholders.
- **Define the risk assessment strategy**.
  This includes the risk assessment process of business initiatives and describes how risks from initiatives will be raised and incorporated into the project risk process as well as overall risk management process. Roles, responsibilities, accountabilities, and authorities should be defined and communicated as part of the risk assessment strategy. Developments in risk assessment and business processes should be evaluated to ensure that risk assessments will provide support for current and future business needs.
- **Define the context of the risk assessment process.**
  Organizations need to identify risks based on events that might prevent, degrade, or delay the achievement of business objectives. This includes a description of stakeholders' perspectives, risk appetite, internal and external policies and standards, and risk categories. The risk categories include the relevant technical areas of the systems and technologies to facilitate identification of risks across the system development life cycle.
- **Define risk thresholds.**
  Leverage risk appetite statement to elaborate the risk thresholds and conditions under which a level of risk may be accepted.
- **Define training and qualification requirements for personnel.**
  The training and qualification include awareness of the risk assessment in its operational environment and a defined program of familiarization. All stakeholders and contributors shall be trained in accordance with the risk management process.
- **Translate technical risk to business risk.**
  Risk items need to be translated to business risk and presented using a business language rather than technical jargon.

4.1.2 Timely risk assessment process and activities

Objective: Complete risk assessments within appropriate time frame acceptable to the business.

Key Results:

- Internal and external risk assessment context and boundaries (e.g. risk appetite, regulatory requirements, internal and external policies) are defined and communicated
- Internal context (policies, standards, procedures, etc.) are mapped into business risk statements in alignment with risk appetite statement
- External context (regulations, industry standards, legal obligations, etc.) are mapped into business risk statements in alignment with risk appetite statement

Activities and Tasks:

- **Define end results and specific activities in risk assessment.**
  List the activities and tasks that should be done during the risk assessment. Ensure dependencies for each activity have been identified.
- **Identify resources.**
  Resources include people, artifacts, materials, and technology needed to complete risk assessment activities. Define the required human resource skill sets.
- **Define the ownership of the responsibility.**
  This ownership implies a commitment to complete the work done by the due date with a standard of quality.
- **Define activity execution approach and traceability.**
  Identify which activities will be performed manually and which ones will be automated. Ensure transparency in activity execution with a clear traceability structure.
- **Set a deadline for each activity.** Establish acceptable amount of time needed to complete each activity in accordance to the scope and resource availability. Ensure escalation procedures are defined for activities that have not been completed on the maximum acceptable time established.

4.1.3 Continuous risk assessment process and activities

Objective: Offer continuous risk assessment services accessible to stakeholders

Key Results:

- Access to risk assessment platform and artifacts to business is provided at all times
- Automated gating decision based on risk profiles with well-defined roles in continuous risk assessment are developed.
- Risk assessment activities are integrated into agile and DevOps ecosystem (deployment pipeline, issue/case management system, CI and CD environment etc.)

Activities and Tasks:

- **Define self-served risk assessment initiation activities.**
  Enable business to initiate risk assessment on a self-served manner by defining risk assessment templates.
- **Define risk assessment integration points and methods for new projects.**
  Enable business to initiate risk assessment activities at defined project phases via manual or automated methods.

4.1.4 Compliance enabled risk assessment process and activities

Objective: The risk assessment ecosystem should comply with all applicable regulations, laws, contracts, policies, and mandatory standards.

Key Results:

- Identify applicable internal policy, standard and procedures that need to be complied with
- Identify applicable external regulations and standards that need to be complied with

Activities and Tasks:

- **Define compliance requirements**.
  Identify regulatory, legislation, and contractual obligations, internal policies, standards and professional guidelines applicable to the organization.
- **Define internal and external change monitoring in regulatory requirements**.
  Changes in the internal and external regulatory requirements might affect the risk. Ongoing monitoring of the regulatory compliance requirements should be performed and reflected on the current and future risk assessments.

4.2 Operational Process Group

The organization shall implement the following activities and tasks in accordance with applicable organization policies and procedures with respect to the operational processes.

4.2.1 Consistent risk assessment process

Objective: Constantly apply standardized procedures and patterns to produce fair and predictable risk assessment results.

Key Results:

- Develop risk assessment templates for each technology profile
- Map each technology decision into business risk statements in alignment with risk appetite statement
- Eliminate inconsistent and subjective risk assessment practices arising from different skillset of risk assessors
- Protect the integrity of the risk assessment to provide assurance that it has not suffered unauthorized modification, duplication, or deletion.

Activities and Tasks:

- **Define risk assessment approach**.
  Risk assessment approach enables different personnel in charge of risk assessment to reach the same results regardless of whoever and whenever conducted risk assessment, provided that they have a certain level of competence in risk assessment and conducted the assessments to the same assets in accordance with the processes and procedures defined in the approach.
- **Define risk assessment inputs.**
  Risk assessment inputs, information and artifacts needed to conduct risk assessment process, should be defined.

- **Define risk assessment outputs.**
  Risk assessment outputs, such as identified risks, risk reports, and risk ratings, should be defined.

4.2.2 Dynamic risk assessment process

Objective: Make risk assessments responsive to changes in threat and vulnerability landscape even after risk assessments are complete.

Key Results:

- Detect new threats and dynamically update the risk assessment with new risks and their associated risk ratings.
- Detect new vulnerabilities and dynamically update the risk assessment with new risks and their associated risk ratings.
- Leverage Threat Intel capabilities and integrate them in the risk assessment ecosystem

Activities and Tasks:

- **Define internal and external vulnerability monitoring activities.**
  Identify, quantify, and prioritize the vulnerabilities that can be exploited by threats to cause harm to assets or to the organization. Vulnerabilities might be arising from external or internal sources need to be monitored continuously. An up to date list of vulnerabilities in relation to assets should be mapped to threats. For each mapped vulnerability and threat, identified controls need to be identified.
- **Define external and internal threat monitoring activities.**
  Threats that have the potential to harm assets should be identified and catalogued. Threat intelligence sources, process and activities need to be defined.
- **Define change monitoring in controls.**
  Existing and planned controls should be identified. Consideration should be given to the possible existing control failures that may jeopardize addressing the risk. Conduct continuous review of controls and assessing whether existing controls are adequate.
- **Re-evaluate the risks.**
  Depending on the changes in the risk context (vulnerabilities, threats, controls, compliance requirements, etc.), trigger the risk assessment process.

4.2.3 Auditable risk assessment process

Objective: The actions of all parties having authorized access to the risk assessment process and artifacts, and the complete chain of events and outcomes resulting from these actions, should be recorded so that this history can be reviewed.

Key Results:

- Which actions needs to be captured in risk assessments that provide an appropriate level of detail on the decision-making rationale and accountability are determined.

- Role-based access with unique identifiers to risk assessment stakeholders are developed. Each entity that will be granted access to risk assessment ecosystem should be uniquely identified.

Activities and Tasks:

- **Define what needs to be audited.**
  Scope of the risk assessment, risk assessment approach, assets, identified risks, risk acceptance criteria, resources involved in risk assessment, resources involved in risk acceptance, resources provided supporting documents, resources who provided information to carry out risk assessments, remediated risks, controls applied to address risk, risk assessment report.
- **Define audit roles and responsibilities.**
  Who will capture the audit trail (format) and in which format should be defined.

4.2.4 Confidential risk assessment process

Objective: Access to risk assessment artifacts should be controlled in accordance with the authorized privileges of the party requesting the access.

Key Results:

- Controls to protect risk assessment information and results against disclosure are identified and implemented
- The privacy of personal information in accordance with relevant privacy or "data protection" legislation to meet the reasonable privacy expectations is protected

Activities and Tasks:

- **Develop risk assessment controls.**
  Controls need to be identified to protect confidentiality and integrity of risk assessment.
- **Secure risk assessment input, output, and traceability trail information.**
  Risk assessment artifacts and associated traceability data should be protected to prevent accidental or deliberate information disclosure and distortion.

4.3 Technology Process Group

The organization shall implement the following activities and tasks in accordance with applicable organization policies and procedures with respect to the technology (operational / business) processes.

4.3.1 Up-to-date risk assessment process

Objective: The risk assessment results provided to stakeholders should be accurate, current and kept up-to-date within a range that has been pre-agreed upon as being applicable to the service being delivered.

Key Results:

- Risk findings remains appropriate to the context of the organization over the time
- Mechanisms to monitor external and internal drivers that can affect the risk are developed
- A notification mechanism to relay changes in the internal and external context with the re-evaluated risks is created

Activities and Tasks:

- **Define currency update responsibilities and authority.**
  Roles and responsibilities should be defined and communicated for implementation of currency updates and maintenance.
- **Develop or acquire knowledge assets.**
  Knowledge assets include system elements, architecture and design, configuration, vulnerabilities, threats, training materials related to domain knowledge, and lessons learned.
- **Share knowledge assets**.
  Knowledge assets should be communicated and shared with all stakeholders transparently across the organization.
- **Implement automated threat intel capabilities.**
  Subscribing threat intel feeds and getting vulnerability notifications will improve threat and vulnerability visibility to knowledge assets.

4.3.2 Measured

Objective: The performance of the risk assessment process should be measured against a variety of desirable performance targets.

Key Results:

- Key metrics that will be collected from risk assessments are developed
- Benchmarks and targets with the collaboration from different stakeholders are established
- Metrics to enhance the posture of cyber risk assessment process and controls are implemented and used.

Activities and Tasks:

- **Define metrics.**
  Identify and implemented risk assessment metrics.
- **Define roles and responsibilities.**
  Identify responsibilities and authority for implementation of metrics development, reporting and maintenance.

4.3.3 Scalable risk assessment process

Objective: Risk assessment ecosystem should be able to grow in its capacity to meet the rising demand for its services offered.

Key Results:

- Capabilities to handle scaling requirements in the case of an increased or expanding workload or scope are developed
- Processing time for the risk assessments and enable concurrency are decreased.

Activities and Tasks:

- **Define scalability requirements.**
  Increased or expanding workload thresholds and timeframes should be identified. To satisfy SLA requirements, adequate resource planning should be procured.
- **Define roles and responsibilities.**
  Responsibilities and authority for implementation of scalability requirements should be identified and communicated.

4.3.4 Customized risk assessment process

Objective: Create re-usable customized risk assessment templates to incorporate organization's internal and external risk drivers including but not limited to different technologies, policies, and regulations.

Key Results:

- Re-usable risk assessment templates that can be selected by business are created
- Feedback from business into risk assessment templates for continual improvement are incorporated

Activities and Tasks:

- **Develop risk assessment domain templates**
  Capture essential common and different features, technologies, capabilities, concepts, and functions that will drive the risk assessment process.
- **Define responsibilities and authority for implementation of customization**.
  Identify roles and responsibilities for creating and updating re-usable risk assessment templates
- **Capture feedback**
  Integrate feedback from all stakeholders to continuously enhance existing and create new customized templates.

5. Terms and Definitions

To support inclusivity of different views and perspectives, it is important to have agreed definitions of the concepts that underpin risk assessment and management. This ensures a common language throughout the process and avoids talking at cross purposes.

Risk assessment - overall process of risk identification, risk analysis and risk evaluation
Risk identification - process of finding, recognizing and describing risk sources and events
Risk analysis - process to comprehend the nature of risk and to determine the level of risk
Residual risk- remaining level of risk after taking into consideration risk mitigation measures and controls in place.
Risk - the effect of uncertainty on objectives. It is the expression of the likelihood and impact of an event with the potential to affect the achievement of an organization's objectives.
Risk capacity - maximum risk an organization can take for any type of business risk.
Risk appetite - the maximum level of risk an organization is willing to take on in order to do business. Amount and type of risk that an organization is willing to pursue or retain. The aggregate level and types of risk that an organization is willing to assume within their risk capacity, in line with their business model, to achieve their strategic objectives.
Privacy risk assessment - overall process of risk identification, risk analysis and risk evaluation with regard to the processing of personally identifiable information (PII). Privacy risk is defined as the “potential loss of control over personal information”
Risk management- systematic approach to setting the best course of action under uncertainty by identifying, assessing, understanding, making decisions on and communicating risk issues.
Risk response- the continuum of measures of risk mitigation or control that are developed and implemented to address an identified risk.
Risk tolerance- the willingness of an organization to accept or reject a given level of residual risk (exposure).
Risk culture - the shared values, attitudes, competencies, and behaviors throughout an organization that shape and influence governance practices and risk decisions.
Threat - an individual, event, or action that has the capability to exploit a vulnerability.
Likelihood - a measure capturing the degree of possibility that a threat will exploit a vulnerability, and therefore produce an undesirable outcome affecting the system.
Impact - result of a threat exploiting a vulnerability, which has a negative effect on the success of the objectives for which we are assessing the risk.

