Risk Acceptance Guidelines

Risk Acceptance

Risk Acceptance (or risk retention) is acknowledging and agreeing to the consequences of a risk exposure. When a risk cannot be eliminated, reduced to an acceptable level or transferred to another source, it may then be accepted. Approval from management must consequently be obtained.

Risk Acceptance Form (RAF)

The Risk Acceptance Form (RAF) shall be used to formally document the acceptance of a risk resulting from any deficiency, exception or deviation from company policy, standards, guidelines, operational processes, and/or internal controls.

It shall also be used to document acceptance of identified risks and vulnerabilities in information security controls, projects, contracts with 3rd party vendors/suppliers or audit findings that may not be readily addressed.

The RAF shall be used in instances where a potential or actual risk to the enterprise is likely to exist regardless of risk severity. The risks identified in the RAF will be inputs to the existing risk registers of the Business Units.

The RAF requires a justification of the risk to be accepted and the compensating controls or remediation plans to address the risk.

A. Process

1. Accomplishing and Submitting the Risk Acceptance Form
   - 1.1. The RAF shall be prepared by the requesting business unit, project owner or jointly with other owners of the risks for acceptance.
   - 1.2. The risk acceptance request should detail and include relevant information that will describe the identified risks.
   - 1.3 The appropriate risk category (Risk Family) must be indicated in the RAF to determine the area where the risk acceptance will have an impact.
   - 1.4 Justification of the risk for acceptance should include the advantages (e.g. benefits) and disadvantages (e.g. loss) if risk is accepted.
   - 1.5 To ensure timely capturing and reporting of risks, the completed RAF should be submitted within seven (7) business days upon identification of the risk(s) for acceptance.

2. Risk Assessment, Controls and Remediation Plan
   - 2.1 Assessment and rating of the risk must include at a minimum, an estimation of the likelihood and impact (financial and non-financial) of the risk. The requesting unit may refer to the Likelihood and Impact Table (Annex A) in the RAF.
   - 2.2 Detailed information on the compensating or alternative controls that will be applied for the risk being accepted must be included in the RAF. Supporting documents if available, must be provided.
   - 2.3 Details of proposed remediation plan and indicate the planned solutions and actions, including proposed timelines to address the risk, or when to apply and improve controls.
   - 2.4 Remediation or action plans to address High or Extreme Risks should be completed within a reasonable timeframe to minimize occurrence of incidents or issues arising from the risk accepted. The actual timeline should be discussed by the Requestor among the Risk Owner, ERM, Compliance, OCISO as appropriate.

2.5 Timelines to resolve risk acceptances from audit findings are discussed separately by the BU with Audit Division.

2.6 Business Units or Risk Owners should note and include in their existing Risk Registers the risks identified in their RAF.

3. Acknowledgement, Acceptance and Clearance

3.1 The RAF must be duly acknowledged and/or approved by the Business Unit Head (e.g. Division Head or Group Head) requesting risk acceptance. As Risk Owners, it is expected that the DH or GH has reviewed the RAF prior to their sign-off.

3.2 A RAF that is not signed-off by the DH and GH concerned will not be accepted.

3.3 For instances that a risk for acceptance will impact another Business Unit, a Subject Matter Expert (SME) from the impacted unit may be required to acknowledge and sign the RAF. An SME will also need to acknowledge the RAF if the risk for acceptance involves a deviation from a policy or control owned by the impacted Business Unit.

3.4 ERM, Compliance, OCISO and Audit will sign the RAF once the evaluation and review of the risk acceptance has concluded.

B. Evaluation and Review of the Risk Acceptance

1. Evaluation of the RAF shall go through the appropriate Governance Units in InLife which includes OCISO, Compliance, ERM and Audit. It may conduct further inquiries with the proponents of the risk acceptance request to calibrate on the risk ratings.
2. If the Risk Acceptance involves a deviation or exception from InLife's Information Security policies, guidelines and procedures, the Chief Information Security Officer must review and sign the form.
3. InLife has no appetite/tolerance for risks that exposes the Company to legal issues and compliance/regulatory breaches. The Chief Legal and Compliance Officer shall review and evaluate RAFs that exposes the Company to such risks.
4. If the Risk Acceptance emanates from the findings of internal and external audit, the RAF must be duly acknowledged and noted by the Chief Auditor.
5. If the Risk Acceptance involves deviations or exceptions on policies owned by the Business Units, the Division Head and Group Head must review and sign the form.
6. Risk Acceptances on Franchise Risk that are rated High to Extreme should go through the President/CEOs approval or veto.

C. Revalidation of the Risk Acceptance

1. The Business Owner is responsible to revalidate, renew or resolve (close) the risks identified in the RAF. A justification for renewal of the risk must be provided following the process indicated in items 2.1 to 2.3 of Sec. A.2. of this Guideline.
2. Revalidation and renewal of the RAF should be performed annually (at a minimum) for Low Risk Ratings. For risk acceptances with Medium, High and Extreme ratings, revalidation will be conducted on a regular/periodic basis as set by ERM.
3. Risk acceptances coming from audit findings shall be managed by Audit Division. These risk acceptances once closed/resolved shall be shared by Audit Division to ERM for recording.

D. Monitoring of Risk Acceptance

1. ERM shall be responsible to monitor and oversee that the Risk Acceptance Guidelines are observed. It is tasked to perform the following;

1.1 Maintain a repository/tracking/log of all submitted RAFs

1.2 Liaise or coordinate with the requesting Busines Unit, SMEs, Risk Owner on matters related to the risk for acceptance during the review and evaluation of the RAF. Including the timely submission of the RAF as required in item 1.5 of Sec A.1 of this Guideline.

1.3 Initiate discussions with OCISO, Compliance and Audit in reviewing and evaluating the risk acceptances.

1.4 Oversee that the annual revalidation of risk acceptances is performed by the Business Units.

1.5 Reporting a monthly summary of Risk Acceptances to OCISO, Compliance, Audit and SFMG Head (as Chief Risk Officer)

1.6 Reporting of High and Extreme rated risk acceptances to the Risk Committee (quarterly or as needed) and to the President and CEO (as needed)

2. ERM owns the company's Risk Acceptance Guidelines and is responsible to develop, improve and cascade to the organization any changes to the Guidelines.

Definition of Terms

The following are the definition of terms used in this Guidelines.

1. Business Unit – refers to Inlife working units e.g. Department, Team, Division, Group

2. Compensating (or Alternative) Controls – a control that is put in place as an alternative to satisfy the requirement for a security or control measure that is deemed too difficult or impractical to implement at the present time.
3. Deficiency – a control or process that is well designed but does not work as intended.
4. Deviation – any change or planned departure from a requirement, process or policy.
5. Exception – a condition that is not aligned with the formal expectations as defined by a policy, standard and/or procedure.
6. Governance Units – refers to the units in the organization that has risk, control, and compliance oversight functions. This refers to ERM, Legal and Compliance and the Office of the Chief Information Security (OCISO). This also includes Audit Division who performs independent assurance reviews of the all the functions.
7. Requesting Business Unit – the unit requesting or filing the Risk Acceptance Request
8. Requestor – refers to the person who initiates the Risk Acceptance Form. For projects, the requestor shall be the project owner/proponent.
9. Risk Acceptance - accepting the identified risk and not taking any other action in order to reduce the risk because its possible impact and consequence can be accepted.
10. Risk Owner – an accountable point of contact for an enterprise risk. Commonly, Risk Owners are at the senior leadership level who coordinates efforts to mitigate and manage the risk with various individuals who owns parts of the risk.
11. Risk Register – repository of the risks logged by each Business Units in their annual risk register updating exercise.
12. Risk Severity – the magnitude of a risk expressed in terms of the combination of likelihood and impact.
13. Subject Matter Expert (SMEs) – an individual that has deep understanding and knowledge of a particular job, process, project, department, function, technology etc.