ERM Post-Incident Assessment

MARCH 2024

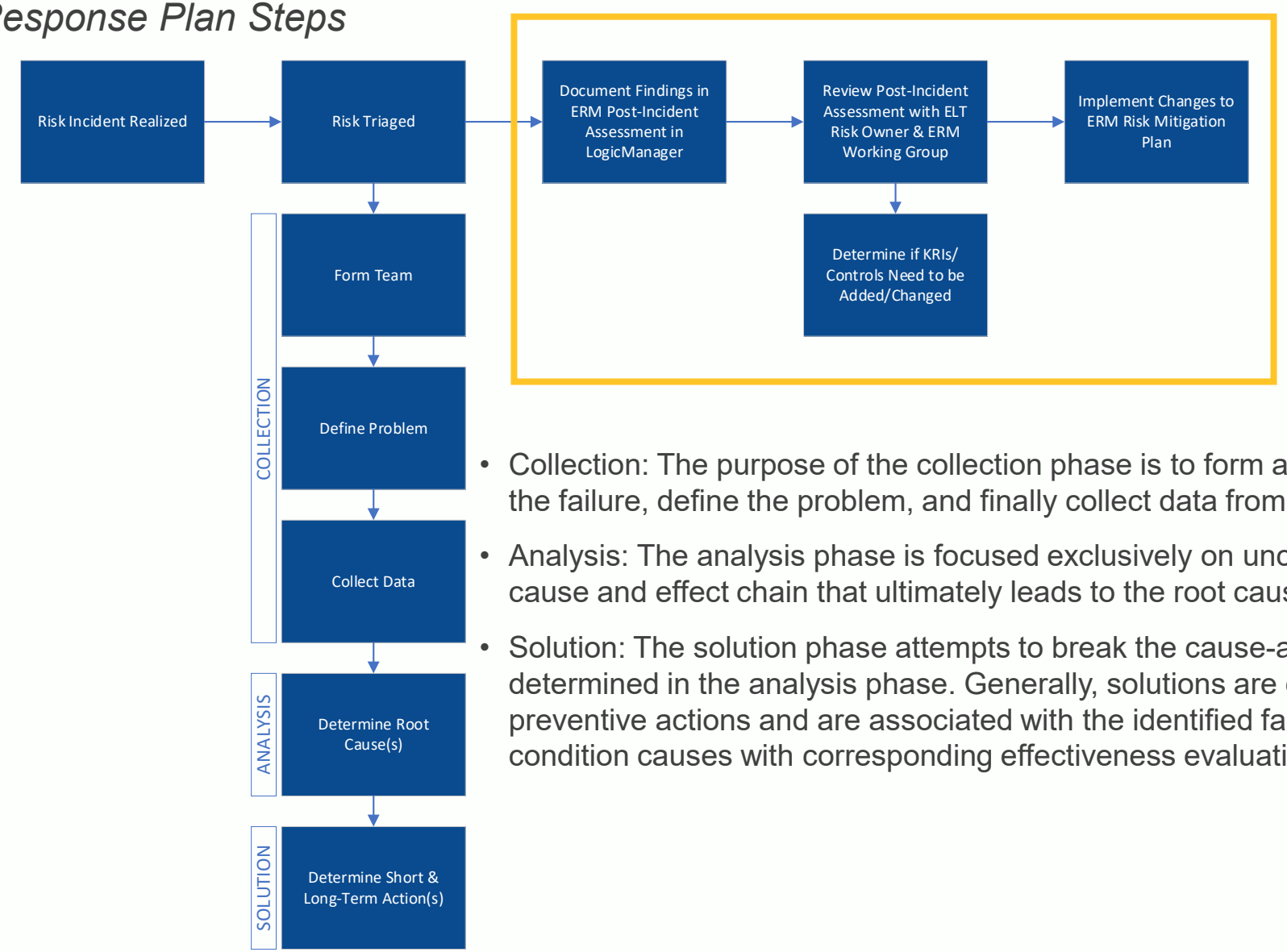
Brink's ERM Program

ERM Post-Incident Assessment

- **Overview**
  - If one of our critical risks materialized, the affected business and/or functional teams would develop and execute a Post-Incident Response Plan.
  - The ERM Program is not responsible for remediation when risks materialize.
  - The ERM Program is responsible for ensuring that critical elements of the Post-Incident Response Plan have been documented in a common framework, so that the relevant ERM stakeholders can assess the effectiveness of Controls and KRIs and evaluate if adjustments need to be made.
- **Procedural Requirements**
  - Once a Post-Incident Response Plan has been completed and a root cause has been identified (or the ELT Risk Owner has determined that most of the short-term actions have been completed), an ERM Post-Incident Assessment form must be submitted in LogicManager within 30 days following the later of (1) finalization of root cause analysis; and (2) relevant ELT member's determination that the near-term remediation of the incident is complete.
    - The ELT Risk Owner is responsible for designating a member of the Risk Response Team or the ERM Risk Working Group to complete the ERM Post-Incident Assessment form.
  - The ELT Risk Owner and ERM Working Group will then have 30 days to review the ERM Post-Incident Assessment in LogicManager and determine if any updates are needed to the Controls and/or KRIs.

Brink's ERM Program

Post-Incident Response Plan Steps



- Collection: The purpose of the collection phase is to form a team to investigate the failure, define the problem, and finally collect data from the incident.
- Analysis: The analysis phase is focused exclusively on uncovering the failure cause and effect chain that ultimately leads to the root cause of failure.
- Solution: The solution phase attempts to break the cause-and-effect chain as determined in the analysis phase. Generally, solutions are corrective and/or preventive actions and are associated with the identified failure action and/or condition causes with corresponding effectiveness evaluations.

Brink's ERM Program

Post-Incident Response Plan Roles & Responsibilities

Role	Responsibilities
Incident Reporter	A person who is familiar with the incident and part of the Incident Response Team and has been designated to liaise with ERM. He/she must promptly contact the ELT Risk Owner associated with the risk incident.
Incident Response Team	Team to define the problem, collect the data, determine root cause and propose short and long-term actions in the development of a Post-Incident Response Plan.
ELT Risk Owner	The ELT Risk Owner designates a member of the Risk Response Team or the ERM Risk Working Group to complete the ERM Post-Incident Assessment form and ensures that the form is submitted within 30 days following the later of (1) finalization of root cause analysis; and (2) relevant ELT member's determination that the near-term remediation of the incident is complete.
ELT Risk Owner, ERM Working Group & ERM Team	This group will receive an email when a new ERM Post-Incident Assessment has been created. Within 30 days of a new ERM Post-Incident Assessment, this group will: 1) Review the documentation in LogicManager and determine if any Controls/KRIs need to be added or changed and 2) Assess what is appropriate to communicate and to which audiences regarding the incident or plans to the ERM risk mitigation plan due to the incident.
Internal Audit or the appropriate compliance area (SoX, Compliance, Security, etc.)	Provide feedback in the assessment and contingency plan to ensure adequate controls are implemented. Once assessment and new plans are in place (if changes occur) Internal Audit will assess incident and contingency plan are adequate to ensure the ERM risk mitigation plan is effective.

Brink's ERM Program

Post-Incident Assessment in LogicManager

- **ERM Risk*:** Choose from the ERM Risk list
- **Risk Incident Name*:** Provide a descriptive name of the incident
- **Risk Incident Summary*:** Summary of what happened including the timeline and departments involved
- **Risk Incident Impact*:** Provide information on the consequences of the realized incident (financial, regulatory, compliance, customer experience, reputational harm, etc.)
- **Triage Team*:** Provide the names of the team designated to perform the collection and analysis of the incident data and determine the solutions
- **Problem Definition*:** Describe the problem that led to the realized incident and how it was detected
- **Data Collection*:** Retrieve, collect and investigate all relevant and available data about the incident including documentation files, initial issues found, preliminary actions taken, personnel or teams involved, and other key information beneficial to identify the root cause
- **Root Cause Analysis*:** Determine the physical, human and/or organizational causes that played a role in the incident, ask the 5 Whys, and establish cause-and-effect relationships to determine the root cause of the event
- **Short-Term Response Actions*:** List the actions taken to respond to the incident for the short-term
- **Long-Term Response Actions***: List the long-term actions (including implementation dates) that need to take place to respond to the incident going forward

Brink's ERM Program

Post-Incident Assessment in LogicManager

Post-Incident Assessment

Please complete this form

Summary

Please provide a descriptive name of the incident in the subject field below

Subject*
Enter text

ERM Risk*
Select option

Risk Incident Summary*
Enter text

Risk Incident Impact
Enter text

Triage Team
Enter text

Problem Definition
Enter text

Root Cause Analysis
Enter text

Short-Term Response Actions
Enter text

Long-Term Response Actions
Enter text

Reported By*
Select user

Reported On*
12/29/2023

Due Date
mm/dd/yyyy