# New Initiative Risk Assessment and New Initiative Approval Process

CTC Enterprise Risk Management

2022

# Agenda and Training Objectives

1. **Overview of the New Initiative Approval Process (NIAP) and associated New Initiative Risk Assessment (NIRA) template**
   - Create an understanding of the NIAP and NIRA processes and their importance to the organization.
   - Overview of the roles and responsibilities of key stakeholders.
   - Understand why timing, quality and completeness of the NIRA is critical to allow the appropriate review, challenge and presentation of significant risks to the Committee for review/approval.

2. **Introduction of the NIRA template**
   - High level exploration of the key elements and expectations involved in creating a NIRA for your initiative.

Please feel free to use the chat during the session for live Q&A!

## SECTION #1

# Overview of New Initiative Approval Process and New Initiative Risk Assessment

# New Initiative Approval Process

**Purpose:** NIAP is a risk management approval process for initiatives which meet defined criteria at the predetermined stages throughout the initiatives lifecycle. *Refer to the appendix for the process flow.*

The NIAP has embedded criteria to determine which initiatives are required to obtain Enterprise Risk Committee (ERC) / Cross-Functional Risk Committee (CRC) approval.

**Key Benefits:**

- Collaborative approach to understanding risks to meet timelines and project milestones.
- A proactive risk management process that is designed to bring significant risks forward for approval and discussion to facilitate informed decision making at the right time.
- Promotes an integrated risk assessment approach across the organization.
- Addresses scenarios when the risks, controls or costs/benefits significantly change through the lifecycle.
- Allows for better transparency and promotes collaboration between key stakeholders and reduces uncertainties.

**What is an Initiative?**

A new business activity, process, product or partnership, and/or any change to an existing business activity, process, product or partnership.

# New Initiative Risk Assessment

**New Initiative Risk Assessment (NIRA) template:**

The NIRA is the risk assessment and documentation component of the NIAP process. The NIRA is a living document that **requires updating throughout the initiative's lifecycle as new risks are identified and as controls are implemented.**

The NIRA is designed to:

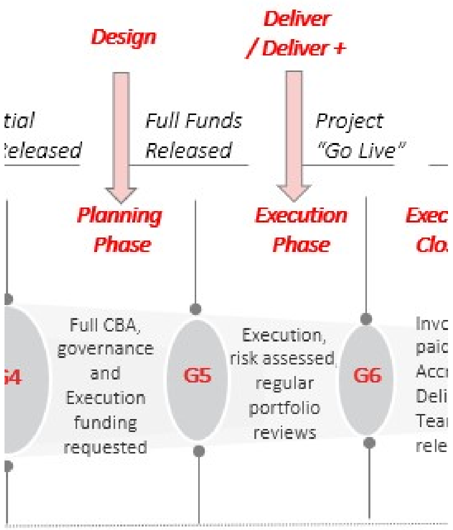
- Capture, identify and assess (enterprise and project) risks of a new initiative and its impacts to business objectives and operations (e.g., think of it as a risk register).
- Centralize the identification and assessment of risks on a standardized template.
- Promote risk discussion and decision capabilities.
- Utilize consistent and standardized risk rating scales.
- Assist Project Managers and Business Owners with identifying and assessing risks, controls, mitigation strategies and to help ensure that all relevant stakeholders are engaged.

**When is a NIRA required?**

All Business initiatives, including key vendor procurement, need to go through the NIRA / NIAP process for proper assessment.

# Completing the NIRA Template

**EIP Gating and NIRA Submission**



** Refer to the Appendix for the complete EIP Gating and Funding Governance Overview.*

**A NIRA will need to be updated to reflect the current state of each key project phase.**

- In accordance with the EIP governance process, a complete and up to date NIRA template must be submitted when entering Execution and before the Go Live. **An initiative should not be Go Live without going through the NIAP process and receiving the proper approvals to move forward.**
- Risks should be added to the NIRA throughout the life cycle of the project and controls should be documented as either 'existing' or as 'controls to be implemented prior to launch'.
- Complete NIRAs must be approved by the Business Owner through email and loaded into Planview.

**Will my initiative need to go to ERC / CRC?**

- At the appropriate phase, NIRAs will be reviewed by Second Line (ERM and Cyber 2nd Line) for ERC / CRC consideration.
- If the initiative involves certain Enterprise level (overriding) risks or a residual risk rating of moderate (or above) it must be presented to the ERC/CRC for information and/or approval.
- To ensure adequate time for review and to minimize delays to the project timeline, a complete NIRA is required **two weeks** prior to the ERC / CRC meeting.

# Roles and Responsibilities

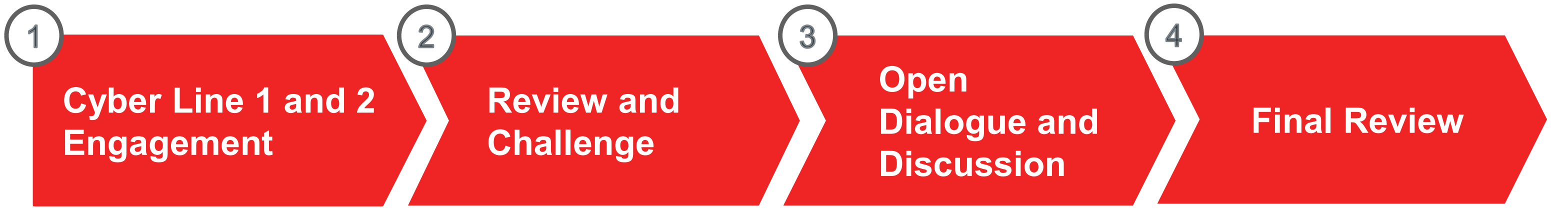
| Key Stakeholder | Roles and Responsibilities |
|---|---|
| **Executive Sponsor** | • Promote accountability and support the adherences of the approval process.<br>• Full awareness and visibility of the initiative and risks identified within the NIRA.<br>• Understand the risks and associated mitigation strategies associated with the initiative. |
| **Business Owner** | • Overall accountability and management of the initiative through the approval process.<br>• Identify and assess the risks, controls, and mitigation strategies within the NIRA template.<br>• Appropriately rate inherent and residual risks.<br>• Coordinate with key stakeholders (e.g. Privacy, Cyber Security, etc.) to gather relevant information and assess risks.<br>• Approve the NIRA and ensure completeness at each of the key stages of the NIAP process.<br>• Complete the NIRA template during the appropriate timeframe and ERC/CRC presentation (if required), with guidance and assistance from the Project Manager. |
| **Project Manager** | • Guide and facilitate the project through the approval process and support the completion of the NIRA template.<br>• Communicate with the Project Management Office during the life cycle of the project and provide a complete NIRA at the appropriate phase(s).<br>• Coordinate with key stakeholders (e.g. Privacy, Cyber Security, etc.) to gather relevant information, where required. |

# Roles and Responsibilities (continued)

| Key Stakeholder | Roles and Responsibilities |
|---|---|
| **Enterprise Risk Committee / Cross-Functional Risk Committee** | • Provide ultimate approval for initiatives which meet certain criteria and consists of Executives and SVPs who meet on a monthly basis.<br>• Full awareness and support of the process and approves any project with residual risk ratings moderate or above, or any overriding (enterprise) risks. |
| ***Second Line of Defence:*** **Enterprise Risk Management (ERM) / Cyber 2nd Line** | • Escalate risks to the appropriate stakeholders.<br>• Monitor that the NIRA methodology and template are being adhered to.<br>• ERM and Cyber Second Line reviews the NIRA at the designated milestones, challenges the risk assessment where appropriate, and makes the determination if it is eligible (meets criteria) for ERC/CRC review and approval. |
| **Security Team** | • Completes the cybersecurity, technology and data/information-related risks as identified under the various functional controls within the NIST cybersecurity framework and the ISO 27001 frameworks for management of security. |
| **Enterprise Project Management Office** | • Act as liaison between Project Managers and Second Line of Defense in the overall NIRA process.<br>• Verify with Project Managers on accuracy of key information (including but not limit to implementation dates, budget, submission status) in Planview.<br>• Ensure the submitted NIRAs are complete and approved in accordance with the Project Management methodology. |
| **Other Key Stakeholders** | • Other key CTC/CTB Stakeholders (including but not limited to Privacy, Business Continuity, Payment Card Industry, Cyber 1st Line / IT Security, Internal Audit Services, Compliance and Legal) should be engaged to support, identify and assess the initiative risks, as required. |

# Process Life Cycle for IT Projects

In addition to the regular NIAP/NIRA process, IT projects are unique in that they require further cyber security assessment and must engage the Cyber Line 1 and 2.



1 Cyber Line 1 and 2 Engagement

- Project teams should engage Cyber L1 & L2 upon receiving the go ahead for their project to start the security architecture and risk assessment work. This will allow for an early triage of the level of involvement from the three lines of defence.

2 Review and Challenge

- Once the architecture and initial risk assessment is complete, Cyber L2 should be re-engaged to perform a review and challenge before the build phase.

3 Open Dialogue and Discussion

- During the build, an open dialogue should be maintained with Cyber L1 & L2 to help ensure that any new risks or changes to existing risks are adequately assessed.

4 Final Review

- Final NIRA and SRA documents should be provided to Cyber L2 at least two weeks before the scheduled ERC for final review.

**What is an IT Project?**

An IT project can be any type of initiative that deals with a component of IT infrastructure, information systems, or computer technology. This includes integrating with, or connecting to, a vendor for third-party services in SaaS, IaaS, PaaS. IT projects also include software development activities, such as programming a simple mobile app, large scale software systems or mainframe applications.

## SECTION #2

# Introduction and live demo of the NIRA template

(including best practices and samples)

# Overcoming Common Challenges

| Section | Issue | How to Improve |
|---|---|---|
| Initiative Details | Description too vague, too high level or overly technical. | • Develop a clear and concise description that is easily understood by someone not familiar with the initiative and articulates the objectives. |
| Overriding (enterprise) Risks | Overriding risks not adequately assessed and/or considered. | • Engage key stakeholders early on to identify and assess risks. If an enterprise risk is identified, details should be reflected in the NIRA.<br>• Refer to the Definitions tab of the NIRA template for further details. |
| Consideration of Key Risk | Not all key risk categories are considered | • All key risk categories should be considered when completing the NIRA. Review the risk considerations tab in the NIRA for key risk categories that should be considered. |
| Identification of Inherent Risks | Risks and consequences not identified, not clearly articulated or are too technical | • Risk statements should be short, succinct and in easy to understand business language. It should also address the consequence ("so what") of the risk |
| Pre-existing risks | Pre-existing risks are not identified as such. | • Document and label risks that are not "net new" to your initiative and whether the initiative exacerbates this risk. If the pre-existing risk is exacerbated by the initiative, the project must develop action plans to mitigate the risk. |
| Assessment of Controls | All controls (current and future) are assessed in the current residual risk rating and/or are not clearly articulated. | • Current controls and control effectiveness rating should only reflect the controls already in place at the particular phase of the NIRA. Future controls should only be considered in the current controls once they are implemented.<br>• Cleary detail what the controls are and how they address the identified risk. |
| IT Security Risks | Other cyber security activities are not completed in the Design phase of the NIRA. | • Risk assessors may be involved with other activities for reviewing security. While other security activities and assessments may assist the risk assessor to identify some risks to 'inform' the NIRA, the NIRA can be completed prior to and independent of other activities. |

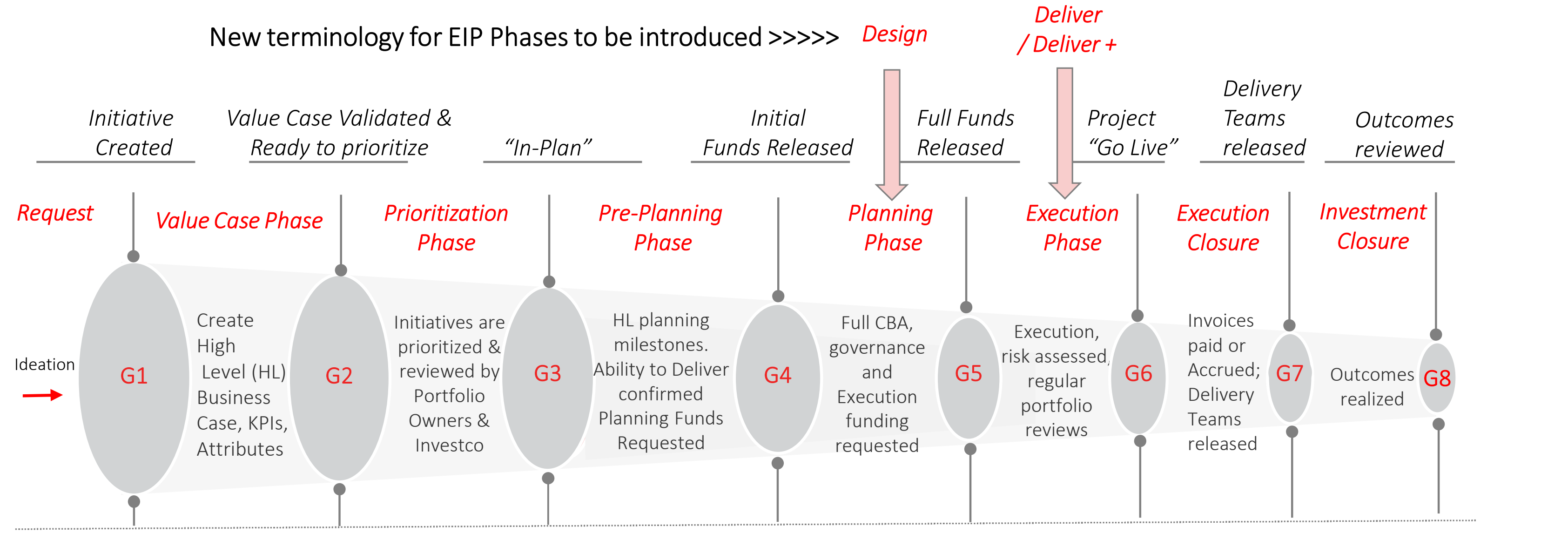
# Appendix

# EIP Gating and Funding Governance Overview

2021 Planned and in-flight investments have been transitioned to the new EIP Gating & Governance process as of June 7th.

- Projects will be 'grandfathered' to their current phase based on the approval status at the time of transition

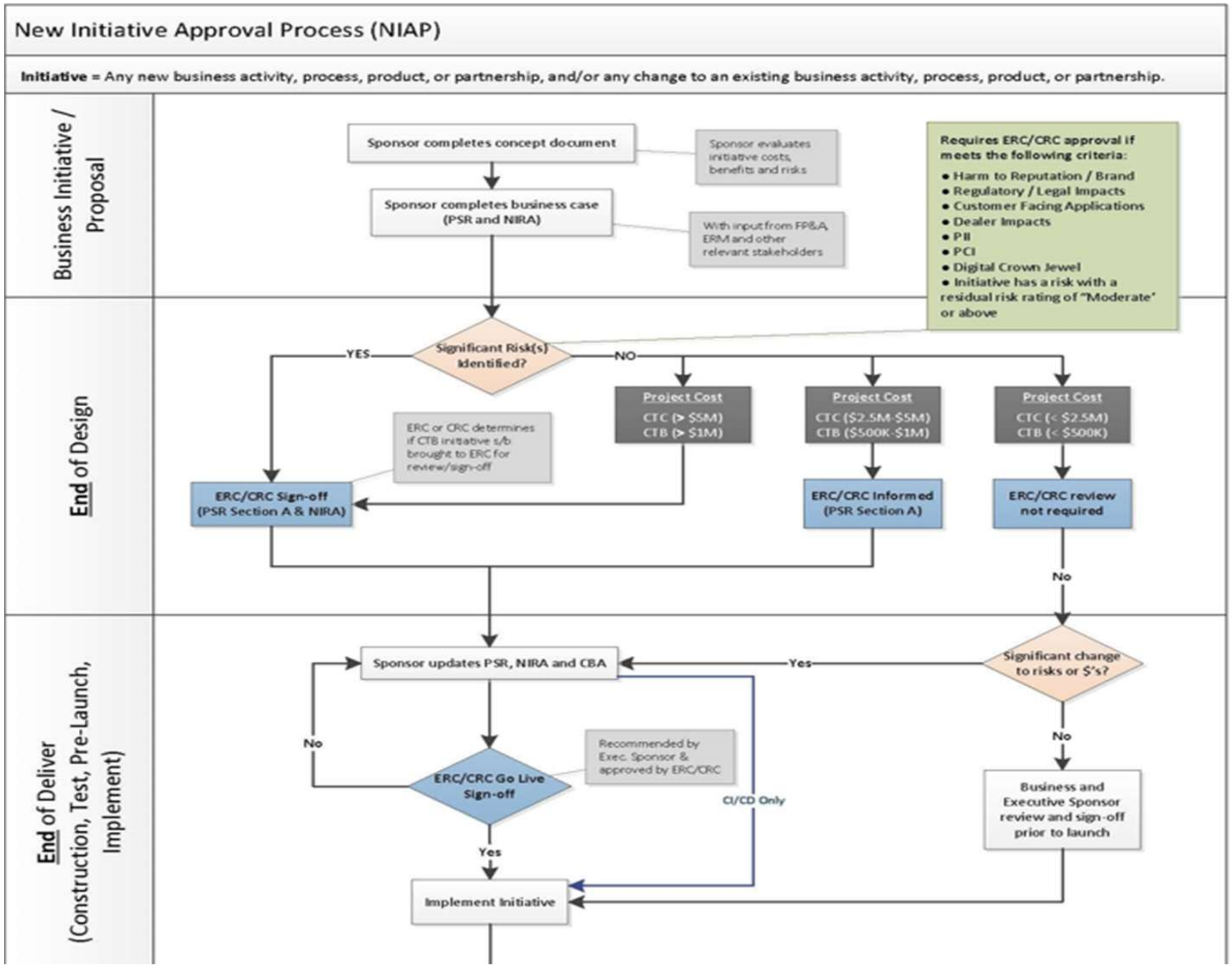
New terminology for EIP Phases to be introduced >>>>>


Design
Deliver / Deliver +
Initiative Created
Value Case Validated & Ready to prioritize
"In-Plan"
Initial Funds Released
Full Funds Released
Project "Go Live"
Delivery Teams released
Outcomes reviewed
Request
Value Case Phase
Prioritization Phase
Pre-Planning Phase
Planning Phase
Execution Phase
Execution Closure
Investment Closure
Ideation
G1
Create High Level (HL) Business Case, KPIs, Attributes
G2
Initiatives are prioritized & reviewed by Portfolio Owners & Investco
G3
HL planning milestones. Ability to Deliver confirmed Planning Funds Requested
G4
Full CBA, governance and Execution funding requested
G5
Execution, risk assessed, regular portfolio reviews
G6
Invoices paid or Accrued; Delivery Teams released
G7
Outcomes realized
G8

| Gating Description | | | | | | | |
|---|---|---|---|---|---|---|---|
| Idea is accepted as a candidate for inclusion in portfolio. | Impact estimate is validated by FP&A, IPT (CBA >=$7M) and Portfolio Owner approves costs and initiative to proceed | Acceptance of initiative into plan. Ranked & prioritized relative to other work | High level planning milestones, ability to deliver. Planning funding approved & released | KPIs, Milestones & NIRA assessed, reviews, FP&A, Portfolio Owner & IPT/Investco (>=$7M) approves spend. Execution funding released | Portfolio reviews to ensure delivery on track. Go Live - Initiative is delivered. *Completed NIRA for implementation | Portfolio Owner approval acknowledges completion of investment closure to support the target business outcome | Post Implementation Review |

- Funnel allows for ideas to be converted to detailed initiatives, which in turn are implemented to capture value
- All initiatives will be tracked in Planview– a single source of truth

# NIAP Process Flow



New Initiative Approval Process (NIAP)

**Initiative** = Any new business activity, process, product, or partnership, and/or any change to an existing business activity, process, product, or partnership.

Business Initiative / Proposal
End of Design
End of Deliver (Construction, Test, Pre-Launch, Implement)
Sponsor completes concept document
Sponsor evaluates initiative costs, benefits and risks
Sponsor completes business case (PSR and NIRA)
With input from FP&A, ERM and other relevant stakeholders
Requires ERC/CRC approval if meets the following criteria:
• Harm to Reputation / Brand
• Regulatory / Legal Impacts
• Customer Facing Applications
• Dealer Impacts
• PII
• PCI
• Digital Crown Jewel
• Initiative has a risk with a residual risk rating of "Moderate" or above
Significant Risk(s) Identified?
YES
NO
Project Cost
CTC (> $5M)
CTB (> $1M)
Project Cost
CTC ($2.5M-$5M)
CTB ($500K-$1M)
Project Cost
CTC (< $2.5M)
CTB (< $500K)
ERC or CRC determines if CTB initiative s/b brought to ERC for review/sign-off
ERC/CRC Sign-off (PSR Section A & NIRA)
ERC/CRC Informed (PSR Section A)
ERC/CRC review not required
No
Sponsor updates PSR, NIRA and CBA
Yes
Significant change to risks or $'s?
No
No
ERC/CRC Go Live Sign-off
Recommended by Exec. Sponsor & approved by ERC/CRC
CI/CD Only
Business and Executive Sponsor review and sign-off prior to launch
Yes
Implement Initiative

Refer to the NIRA template for the full NIAP Process flow.

# Key Contacts

| Department | Primary Contact | Secondary Contact |
|---|---|---|
| CTC ERM | **James Chan**<br>James.Chan01@cantire.com | **Michele Cox**<br>Michele.cox@cantire.com |
| | **CTC ERM General Inbox**<br>ctcerm@cantire.com | **Facebook at Work:** CTC Enterprise Risk Management |
| CTB ERM | **Matt Walker**<br>Matt.walker01@ctfs.com | **Julie Narciso**<br>Julie.Narciso@ctfs.com |
| CTC Cyber Line 2 | **Terence Lam**<br>Terence.Lam@cantire.com | **Max Sakalauskas**<br>Max.Sakalauskas@cantire.com |
| CTB Cyber Line 2 | **Lorri Larstone**<br>Lorri.Larstone@ctfs.com | |
| Enterprise Project Management Office | **Tammy Dodd**<br>Tammy.dodd@fglsports.com | **Gurkeet Lalli**<br>Gurkeet.Lalli@fglsports.com |
| Privacy (PII Risks) | **Alton Williams**<br>Alton.Williams@cantire.com | **Patricia Carswell**<br>Patricia.Carswell@cantire.com |
| Payment Card Industry (PCI Risks) | **Nancy Wood**<br>Nancy.wood@cantire.com | **Mike Williams-Yeagers**<br>Mike.WilliamsYeagers@ctfs.com |
| IT Security | **Christopher Petch**<br>Christopher.Petch@cantire.com | **Marie-Eve Laplante**<br>Marieeve.Laplante@cantire.com |