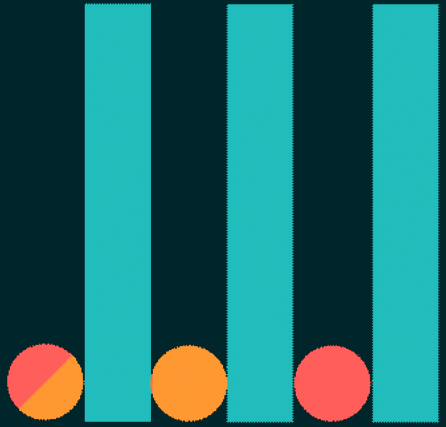
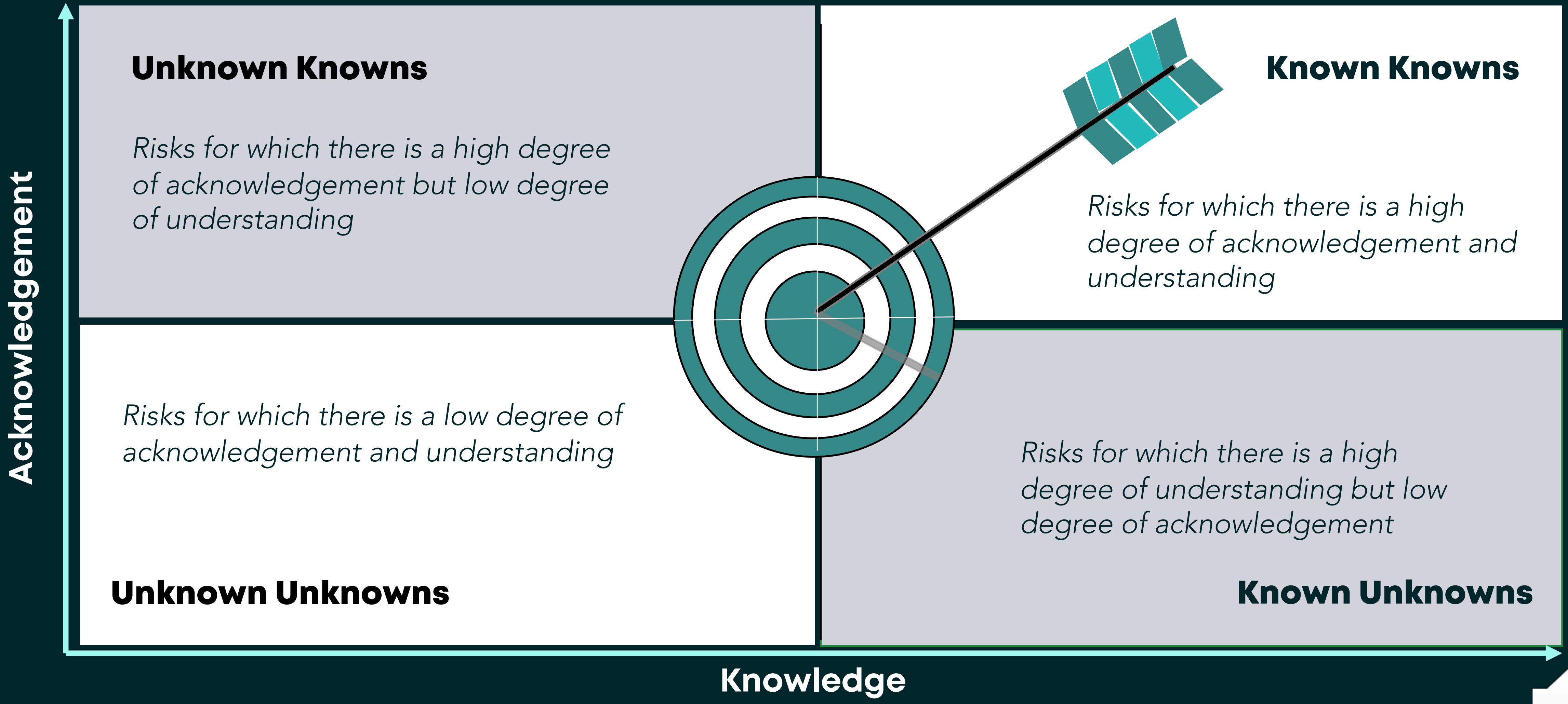


01

RISK AND CONTROL ASSESSMENT LIFE-CYCLE

RECAP

Focus on the unknowns to add value



Unknown Knowns

Risks for which there is a high degree of acknowledgement but low degree of understanding

Known Knowns

Risks for which there is a high degree of acknowledgement and understanding

Risks for which there is a low degree of acknowledgement and understanding

Unknown Unknowns

Risks for which there is a high degree of understanding but low degree of acknowledgement

Known Unknowns

Acknowledgement

Knowledge

WEEK 3

What is a Risk & Control Self Assessment (“RCSA”)?

An RCSA is a systematic and repeatable process to consistently assess inherent operational risks, effectiveness of their associated controls, and enable understanding of operational risk profile (i.e., aggregate residual operational risk). There are 3 types of RCSA:

- Strategic-based RCSA
- Business Unit-based RCSA
- Process-based RCSA

In addition to the above RCSA types, other Risk Assessments are used in the ORMF*, for example:

- New Initiative Risk Assessment
- Third-Party Risk Assessment
- Business Impact Assessments

There are numerous others, including Privacy Impact Assessments, Information Security Risk, IT Risk Assessments, Threat Risk Assessments, etc

WEEK 3

There are a variety of RCSAs that can be leveraged

The following is an illustrative list of key types of RCSAs that are observed in industry:

Strategic RCSA

Scope is focused on identifying the top operational risks that could prevent enterprise achievement of strategic objectives.

Performed in conjunction with the annual strategic business planning process or as a result of elevated strategic risk.

Results inform review/refresh of Operational Risk Appetite & Tolerance.

Facilitated cross-functional workshop with accountable executives.

Business Unit

Scope is driven by mapping key risks and controls to the organizational hierarchy.

Performed by the business units using a variety of methods (workshops, refresh, surveys).

Results form the basis of Business/Segment view of Operational Risk Profile.

Process-Based

Scope is driven by process workflows. Key risks and controls are mapped to each stage of the business process workflows.

Benefits of pRCSA: enables identification of potential blind spots that may exist associated with critical handoffs and dependencies between units and the supply chain.

Results form the basis of Service-Based Operational Risk Profile and of Operational Resilience Posture.

Performed by process owners using a variety of methods (workshops, refresh, surveys).

Deep-Dive

Scope is driven by trigger events (e.g., material ORE, incident, regulatory change) or identification of emerging risk.

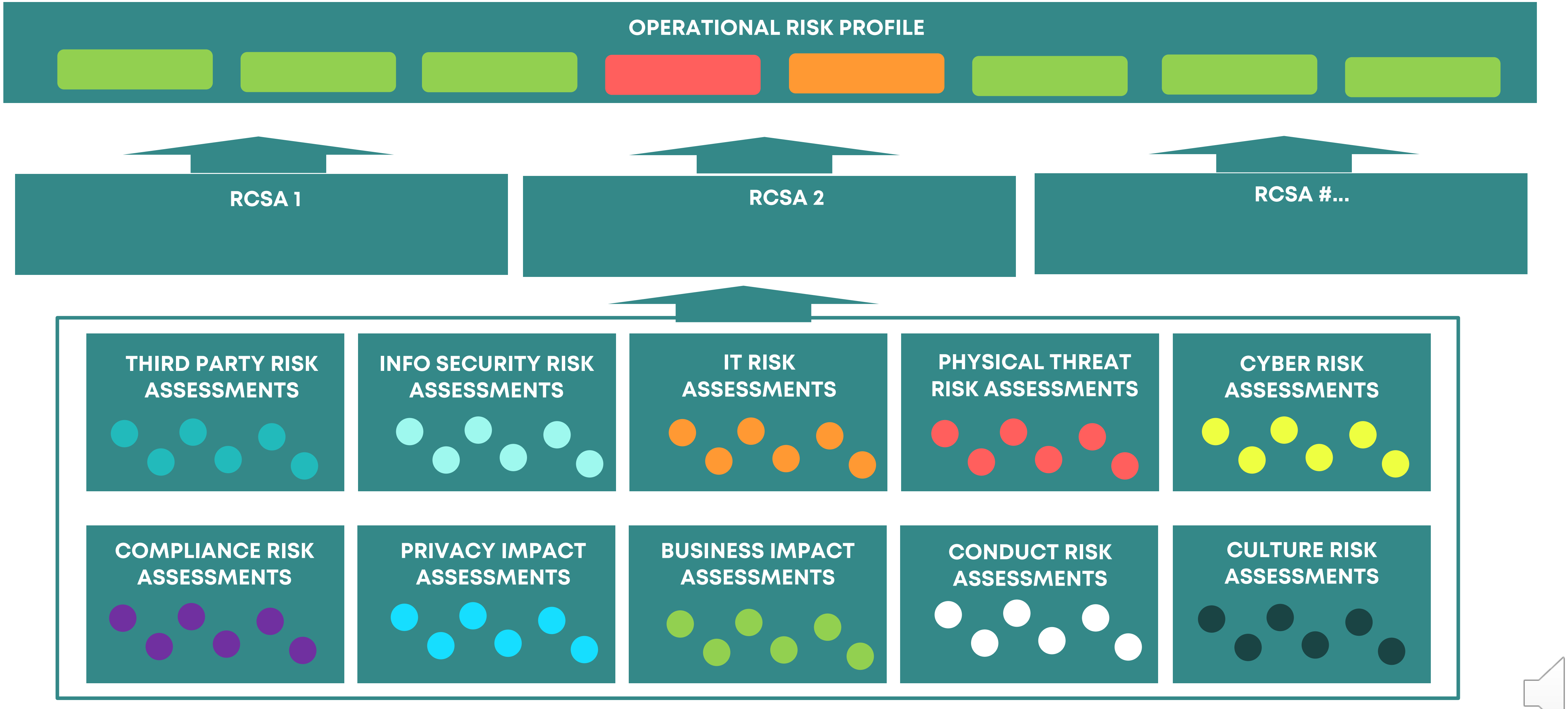
The RCSA focuses on BUs, Processes, and Risks associated or potentially impacted by the trigger event.

The objective is to ensure controls remain adequate to manage operational risk within risk appetite.

Results inform decision-making and are used an input to the Operational Risk Profile.

WEEK 3

What is the relationship amongst the operational risk assessments?



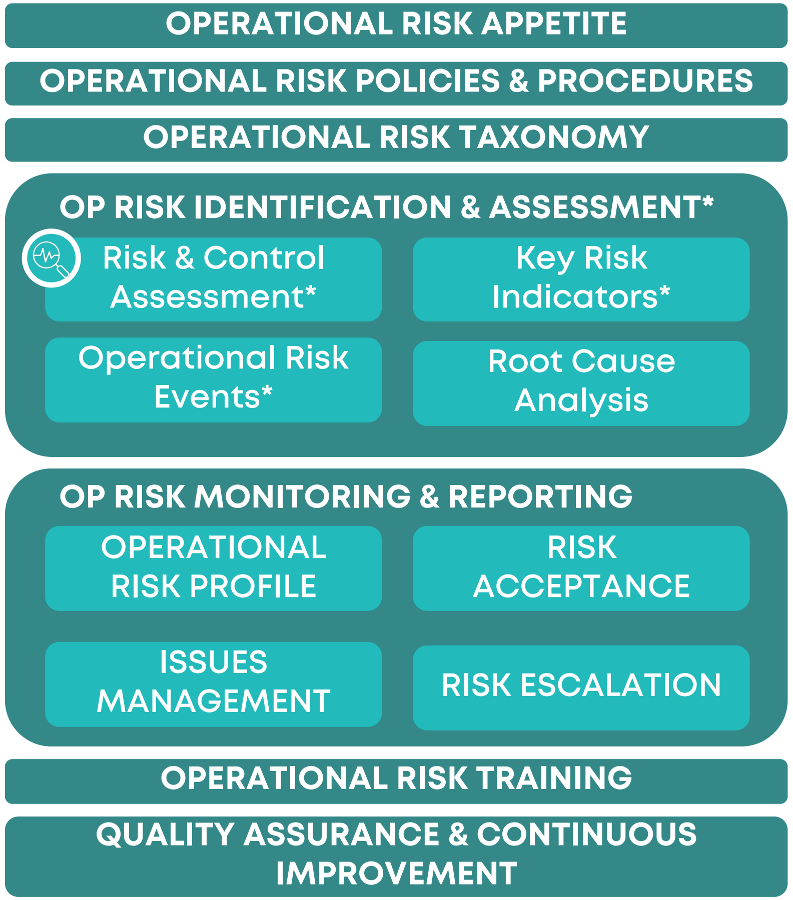
OPERATIONAL RISK PROFILE
RCSA 1
RCSA 2
RCSA #...
THIRD PARTY RISK ASSESSMENTS
INFO SECURITY RISK ASSESSMENTS
IT RISK ASSESSMENTS
PHYSICAL THREAT RISK ASSESSMENTS
CYBER RISK ASSESSMENTS
COMPLIANCE RISK ASSESSMENTS
PRIVACY IMPACT ASSESSMENTS
BUSINESS IMPACT ASSESSMENTS
CONDUCT RISK ASSESSMENTS
CULTURE RISK ASSESSMENTS

RECAP

OSFI E-21 RCSA principles

PRINCIPLE 7

The FRFI should ensure comprehensive identification and assessment of operational risk using appropriate operational risk management practices.



OPERATIONAL RISK APPETITE

OPERATIONAL RISK POLICIES & PROCEDURES

OPERATIONAL RISK TAXONOMY

OP RISK IDENTIFICATION & ASSESSMENT*

Risk & Control Assessment*

Key Risk Indicators*

Operational Risk Events*

Root Cause Analysis

OP RISK MONITORING & REPORTING

OPERATIONAL RISK PROFILE

RISK ACCEPTANCE

ISSUES MANAGEMENT

RISK ESCALATION

OPERATIONAL RISK TRAINING

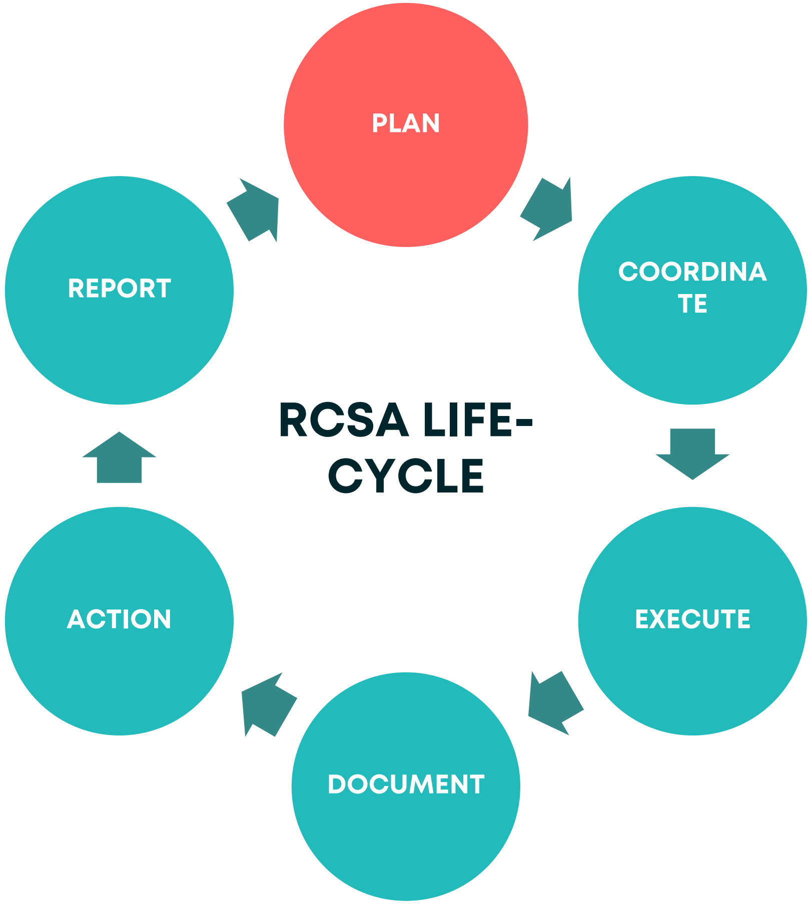
QUALITY ASSURANCE & CONTINUOUS IMPROVEMENT

RCAs are performed

- *Use a self-assessment tool, such as the RCA, to effectively manage operational risks*
- *Apply the RCA to various levels, where appropriate, while taking into consideration proportionality and criticality*
- Use RCAs to assess operational risks and the design and effectiveness of mitigating controls
- RCAs should reflect the current environment and be forward-looking in nature
- Reassess RCAs in response to undertaking significant change or in response to a significant operational risk event
- Where residual risk exceeds the limits and thresholds for operational risk, undertake corrective measures or formally accept the risk, formally documenting the rationale and approval for risk acceptance
- Track, monitor, and subject to independent challenge any action plans resulting from completed RCAs to ensure required enhancements are appropriately implemented and effective

RCSA LIFE-CYCLE

PHASE 1 - PLAN



OBJECTIVES

The key objectives of the RCSA planning phase are to:

- *Determine the nature, scope, frequency, and timing of the RCSAs to be completed over a multi-year-planning period*
- *Identify and confirm RCSA stakeholders and participants*
- *Ensure adequate coverage of the Operational Risk Universe*
- *Avoid overlap and duplication of efforts*
- *Identify and prioritize competing priorities*
- *Establish and communicate to all stakeholders, a comprehensive risk-based RCSA Plan that will be used to monitor progress against*

kMRC

PHASE 1 - PLAN

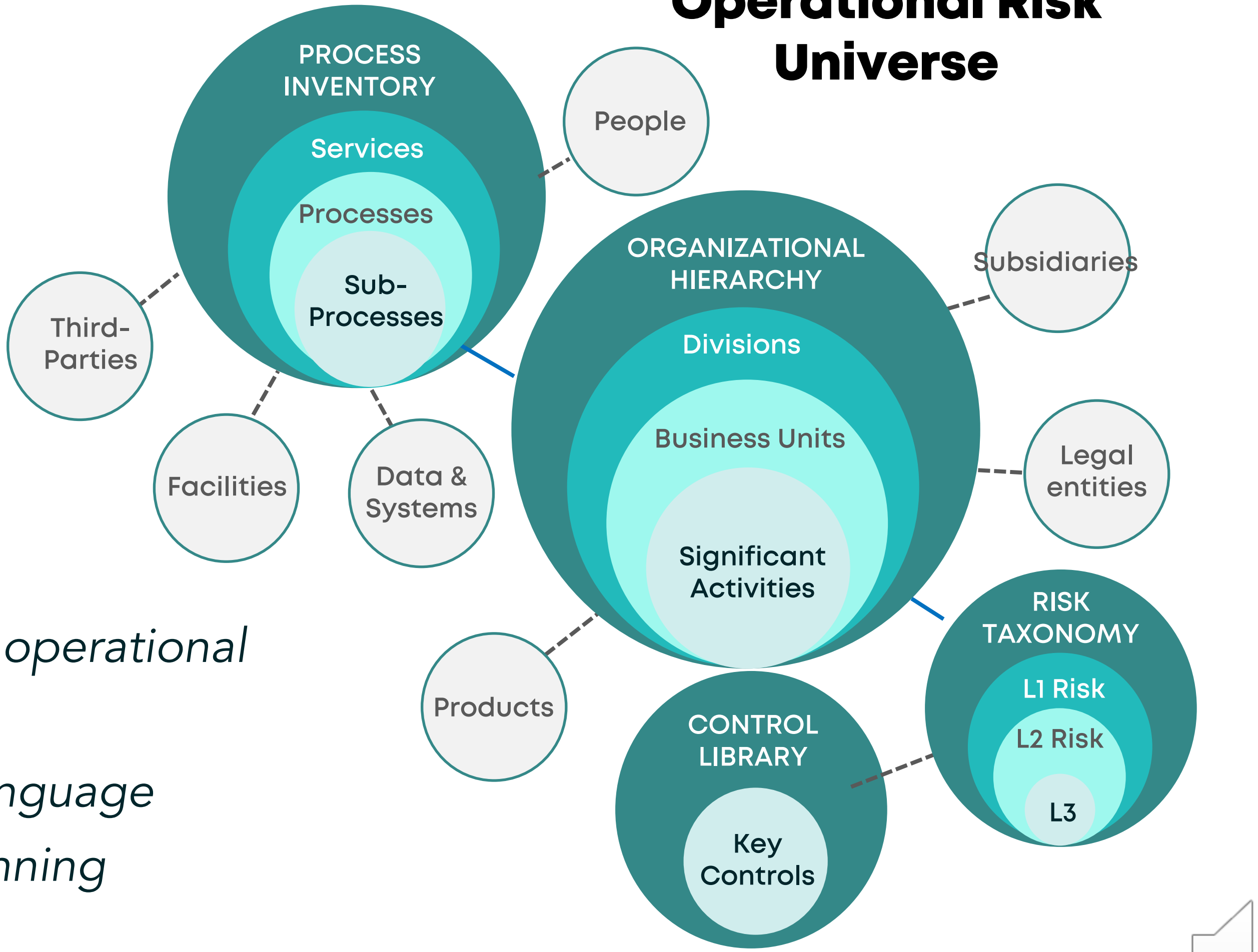
The key objective of the planning phase is to ensure optimal coverage of the operational risk universe

BENEFITS

The key objectives and benefits of using a common and aligned Operational Risk Universe within all operational risk assessments, including the RCSA are to:

- *Enable aggregation and disaggregation of operational risk assessment data from across functional domain areas;*
- *Enable efficient comparative analysis*
- *Reduce duplication of efforts across functional operational risk domains and within the AUs*
- *Promote a common organizational view and language*
- *Streamline and coordinate risk assessment planning*

Operational Risk Universe



kMRC

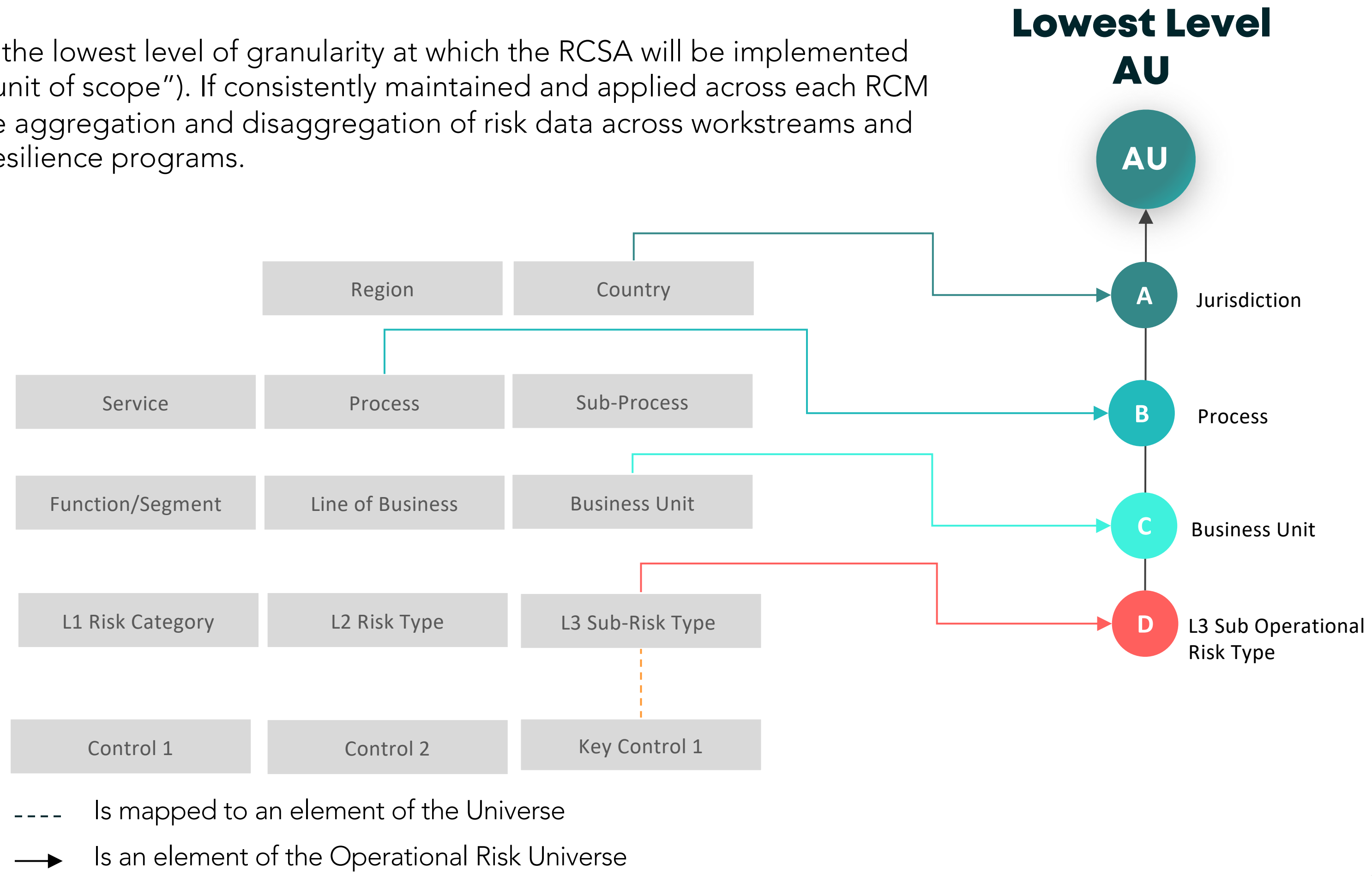
PHASE 1 - PLAN

Carve the Operational Risk Universe into clear and distinct units of assessment ("AUs")

INPUTS

- A Jurisdiction
- B Organizational Hierarchy
- C Process Inventory
- D Operational Risk Taxonomy
- E Internal Control Library

The "AU" represents the lowest level of granularity at which the RCSA will be implemented (i.e., it is the lowest "unit of scope"). If consistently maintained and applied across each RCM element, it will enable aggregation and disaggregation of risk data across workstreams and Operational Risk & Resilience programs.



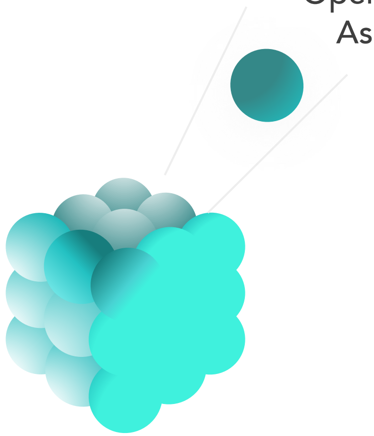
---- Is mapped to an element of the Universe

→ Is an element of the Operational Risk Universe

PHASE 1 - PLAN

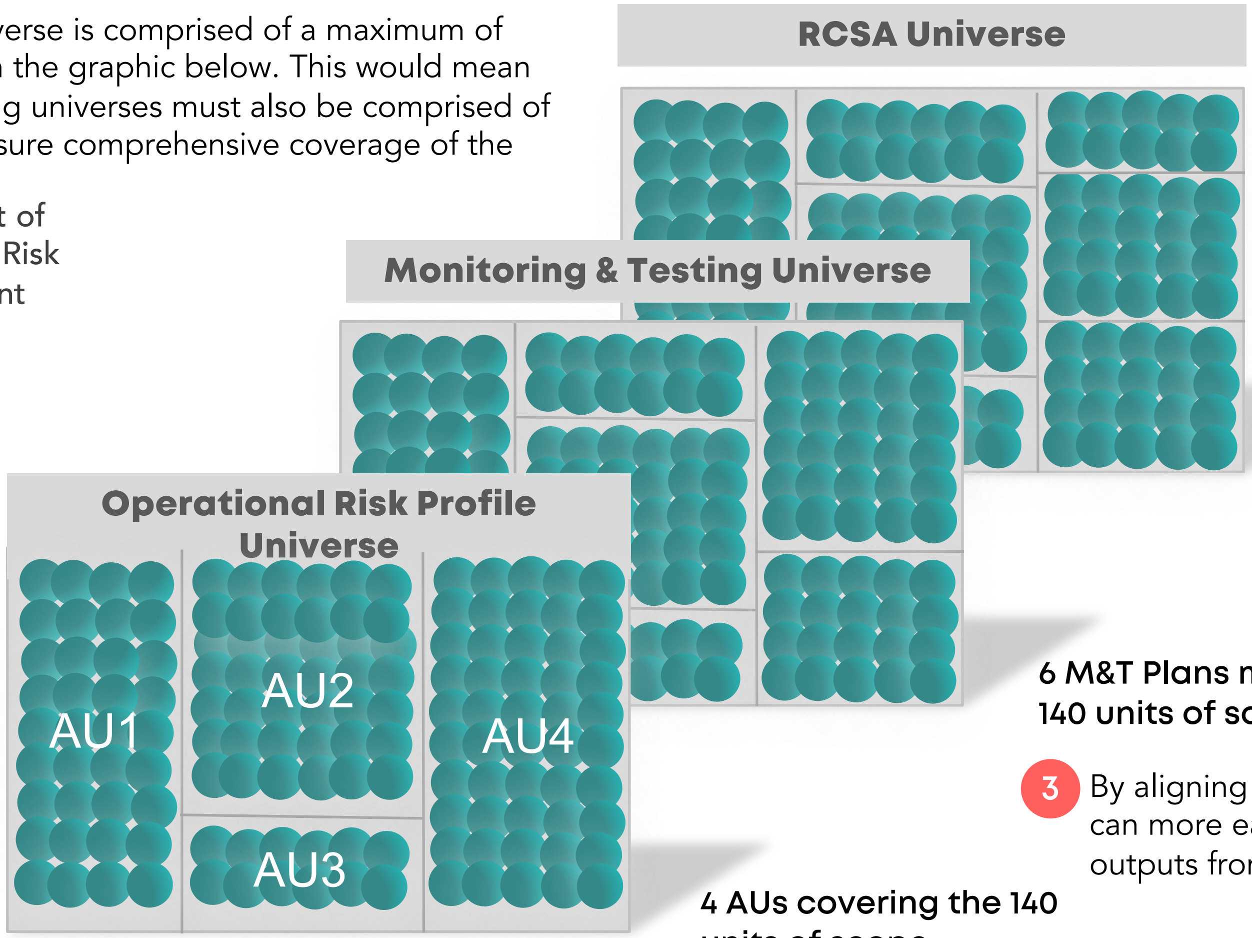
Organize and group the lowest level units of scope into higher level Assessable Units (“AUs”)

1 Let’s say our Operational Risk Universe is comprised of a maximum of 140 units of scope, as illustrated in the graphic below. This would mean that the RCSA, M&T, and Reporting universes must also be comprised of the same 140 units of scope to ensure comprehensive coverage of the Universe.



Lowest Unit of Operational Risk Assessment

Operational Risk Universe = 140 Units of Scope



RCSA Universe

Monitoring & Testing Universe

Operational Risk Profile Universe

2 While all 140 units must be represented, each program can determine how to group them into larger units of assessment, as based on the nature, size, risk and complexity of each unit of scope.

8 Aus (i.e., 8 RCSAs will be completed to cover the 140 units of scope)

6 M&T Plans must be established to cover all 140 units of scope)

4 AUs covering the 140 units of scope

3 By aligning on the lowest unit of assessment, we can more easily aggregate and disaggregate the outputs from execution of the ORMF.

PHASE 1 – PLAN

Determine the nature, frequency, and timing of each RCSA to be performed over a pre-determined period

When developing the RCSA Plan, you should also determine what type of RCSA is required, considering the size, risk, and complexity of the AU. Let's explore the different types of RCSA hat are available and the key factors to consider when determining which is the most appropriate.

	DESCRIPTION	WHEN TO USE IT
CROSS-FUNCTIONAL WORKSHOP	Refers to A 2LOD facilitated workshop with participants from more than one AU that rely on the same controls (e.g., to avoid duplication of effort in assessment common controls)	• At time of initial baseline RCSA (i.e., the first time a RCSA is being done in an AU) • In response to material trigger event impacting multiple AUs
AU WORKSHOP	Refers to a 1B facilitated workshop with first line participants from a specific AU, and support from subject matter experts, as needed	• At time of initial baseline RCSA (i.e., the first time a RCSA is being done in an AU) • In response to identification of high-severity issue(s)
RCSA REFRESH	Refers to 1B updating one or more sections of the RCSA to address a trigger event but without having to update all sections of the RCSA. This may be performed with or without a workshop, depending on the nature and materiality of the trigger event.	• In response to a material trigger event • In accordance with the RCSA cycle of frequency
SURVEY	Refers to 1B execution of the RCSA that is performed without a workshop (desk update)	• Low risk AUs • In accordance with the RCSA cycle of frequency and in absence of a material trigger event

Let’s examine some examples of Trigger Events

A Trigger Event is defined as an event that could have a material impact on either the inherent risk or quality of controls. A Trigger Event can be internal or external. Let’s examine the different types of Trigger Events and what needs to be updated in response.

Material Operational Risk Event

On October 17th, the firm experienced a widespread CHESS system outage affecting critical services affecting multiple business units. Please indicate whether the impacted AUs need to update each of the following elements of the RCSA, in response to the Trigger Event:

RCSA UNIVERSE	RCSA PLAN	INHERENT RISK ASSESSMENT	AU PROFILE	CONTROL ASSESSMENT
YES	YES	YES	YES	YES
NO	NO	NO	NO	NO

Let’s examine some examples of Trigger Events

Internal Audit Issue

Internal Audit raised material concerns regarding the effectiveness of one of the key controls associated with your AU. For each of the elements of the RCSA below, please indicate whether it requires updating, in response to the Trigger Event:

RCSA UNIVERSE	RCSA PLAN	INHERENT RISK ASSESSMENT	AU PROFILE	CONTROL ASSESSMENT
YES	YES	YES	YES	YES
NO	NO	NO	NO	NO

Let’s examine some examples of Trigger Events

New Product

You have received approval to launch a new initiative to introduce a new reverse mortgage product. For each of the elements of the RCSA below, please indicate whether it requires updating, in response to the Trigger Event:

RCSA UNIVERSE	RCSA PLAN	INHERENT RISK ASSESSMENT	AU PROFILE	CONTROL ASSESSMENT
YES	YES	YES	YES	YES
NO	NO	NO	NO	NO

Let’s examine some examples of Trigger Events

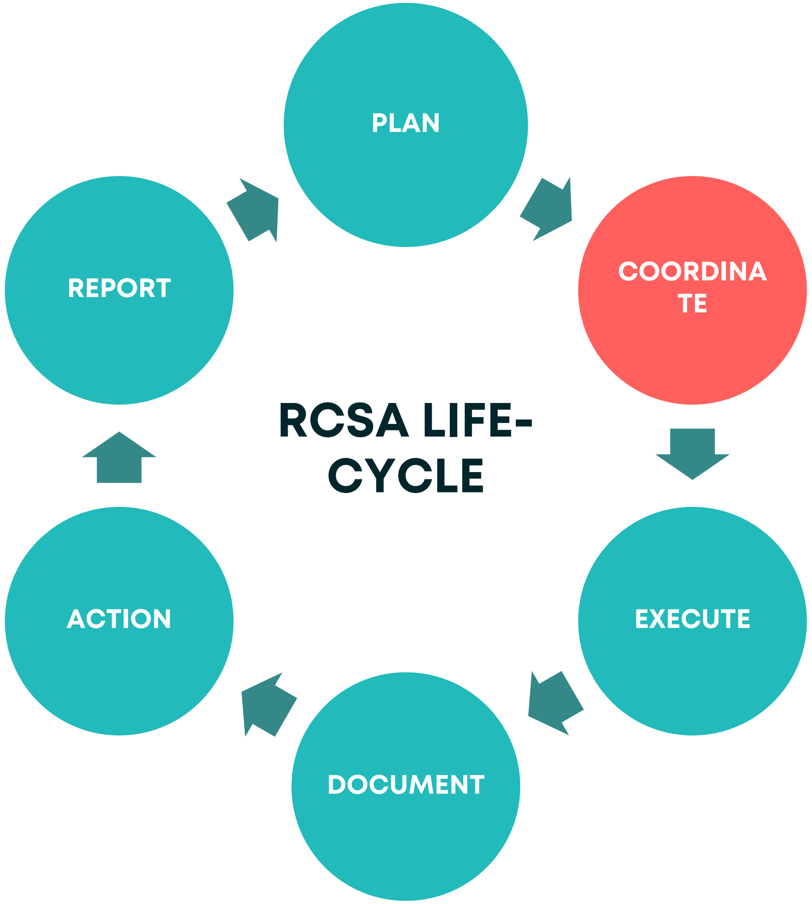
External Event

One of our peers notified us about a recent sophisticated ransomware attack on their firm that leveraged AI for highly targeted social engineering of senior executives. The attackers employed AI algorithms to analyze publicly available information and craft convincing phishing messages that specifically targeted key employees within the organization. For each of the elements of the RCSA below, please indicate whether it requires updating, in response to the Trigger Event :

RCSA UNIVERSE	RCSA PLAN	INHERENT RISK ASSESSMENT	AU PROFILE	CONTROL ASSESSMENT
YES	YES	YES	YES	YES
NO	NO	NO	NO	NO

RCSA LIFE-CYCLE

PHASE 2 - COORDINATE



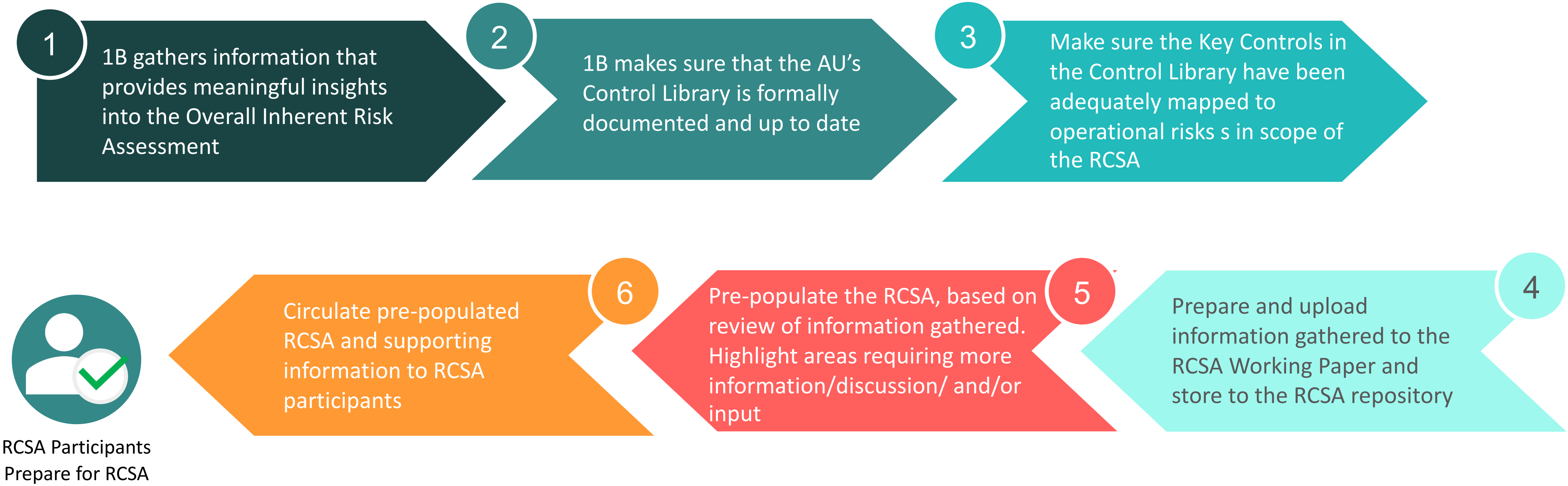
OBJECTIVES

- Ensure the right stakeholders participate in the RCSA
- Ensure RCSA participants are well-prepared and equipped with the information needed to yield meaningful RCSA insights
- Ensure RCSAs are performed using the most recent, relevant, and up-to-date information available
- Enable consistent and efficient execution of the RCSAs

kMRC

PHASE 2 – COORDINATE

The key objective of the coordinate phase is to make sure the right stakeholders are available and prepared to execute the RCSA



1 1B gathers information that provides meaningful insights into the Overall Inherent Risk Assessment

2 1B makes sure that the AU’s Control Library is formally documented and up to date

3 Make sure the Key Controls in the Control Library have been adequately mapped to operational risks s in scope of the RCSA

4 Prepare and upload information gathered to the RCSA Working Paper and store to the RCSA repository

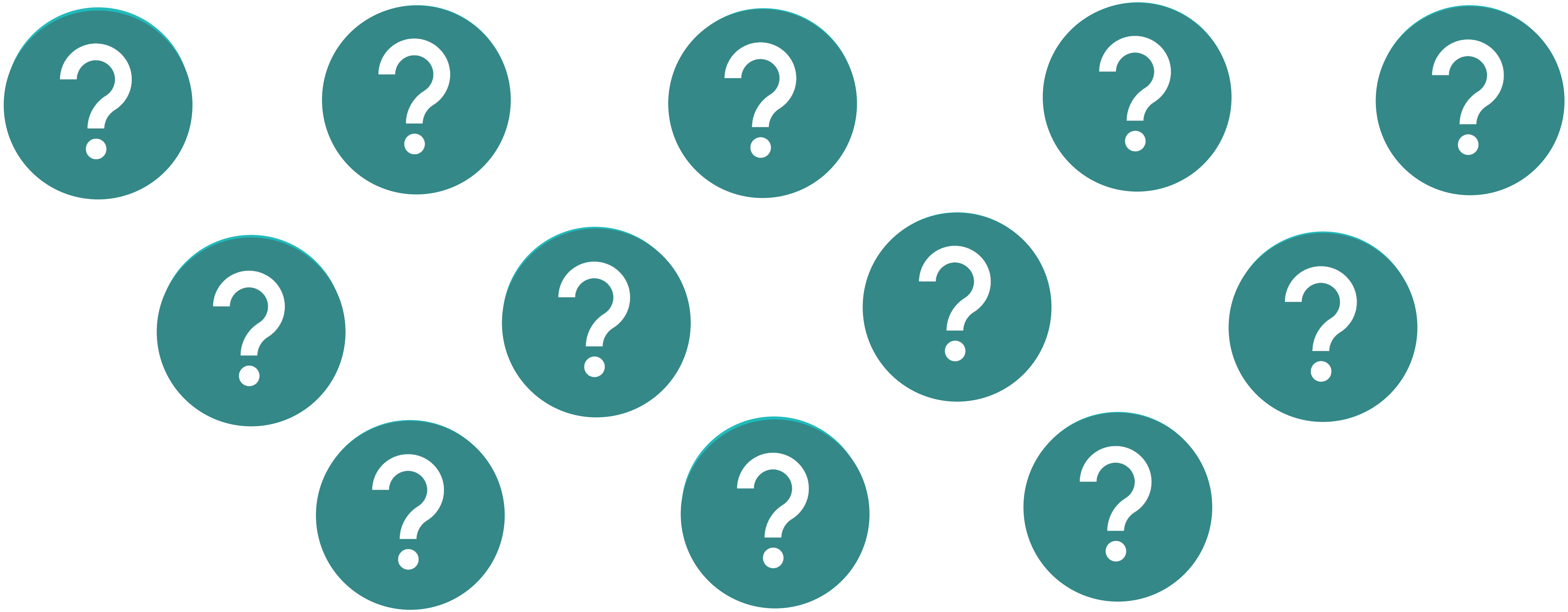
5 Pre-populate the RCSA, based on review of information gathered. Highlight areas requiring more information/discussion/ and/or input

6 Circulate pre-populated RCSA and supporting information to RCSA participants

RCSA Participants Prepare for RCSA

Identifying sources of data for the RCSA

What are some of the sources of data that can be used to prepare for ? Let's hear your ideas and see if they're on the board.



Who should be invited to participate in an RCSA workshop? Uncover them all before time runs out.

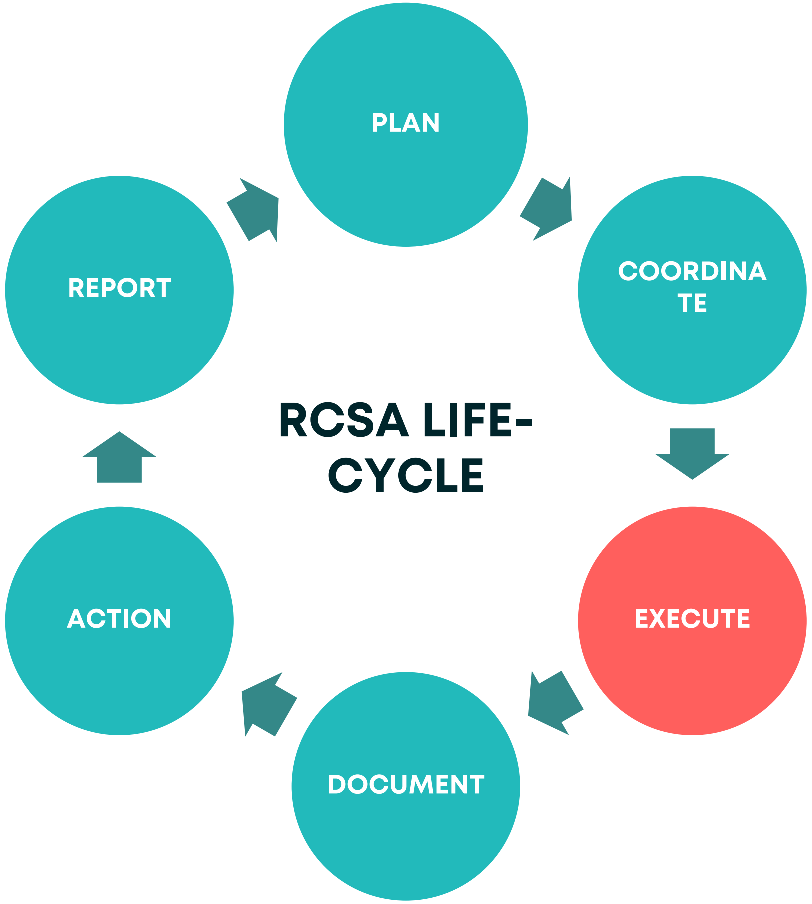
1	2	3	4	5
6	7	8	9	10
11	12	13	14	15

What are some of the key characteristics of an effective RCSA participant? Uncover them all before time runs out.

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15

RCSA LIFE-CYCLE

PHASE 3 – EXECUTE



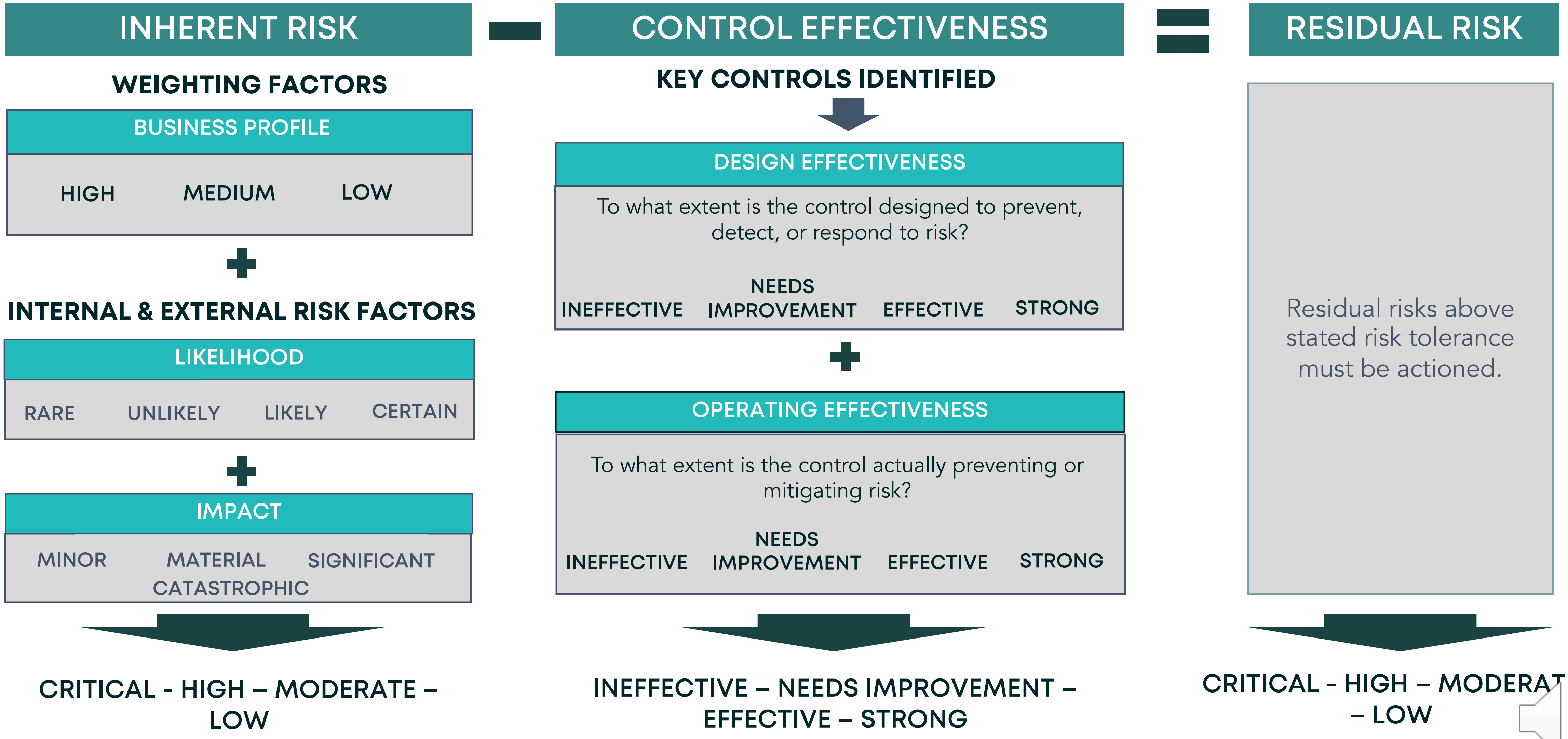
OBJECTIVES

- Determine the AU Profiled Rating
- Determine Overall Inherent Risk Ratings for each of the in-scope RTGs
- Determine Overall Control Effectiveness Ratings for each of the in-scope Key Controls
- Determine Residual Risk Ratings for each of the in-scope RTGs
- Determine the Overall Residual Risk Rating for the AU

kMRC

PHASE 3 - EXECUTE

Illustrative example of an RCSA formula



INHERENT RISK − CONTROL EFFECTIVENESS = RESIDUAL RISK

WEIGHTING FACTORS

BUSINESS PROFILE

HIGH MEDIUM LOW

+

INTERNAL & EXTERNAL RISK FACTORS

LIKELIHOOD

RARE UNLIKELY LIKELY CERTAIN

+

IMPACT

MINOR MATERIAL SIGNIFICANT CATASTROPHIC

CRITICAL - HIGH – MODERATE – LOW

KEY CONTROLS IDENTIFIED

DESIGN EFFECTIVENESS

To what extent is the control designed to prevent, detect, or respond to risk?

INEFFECTIVE NEEDS IMPROVEMENT EFFECTIVE STRONG

+

OPERATING EFFECTIVENESS

To what extent is the control actually preventing or mitigating risk?

INEFFECTIVE NEEDS IMPROVEMENT EFFECTIVE STRONG

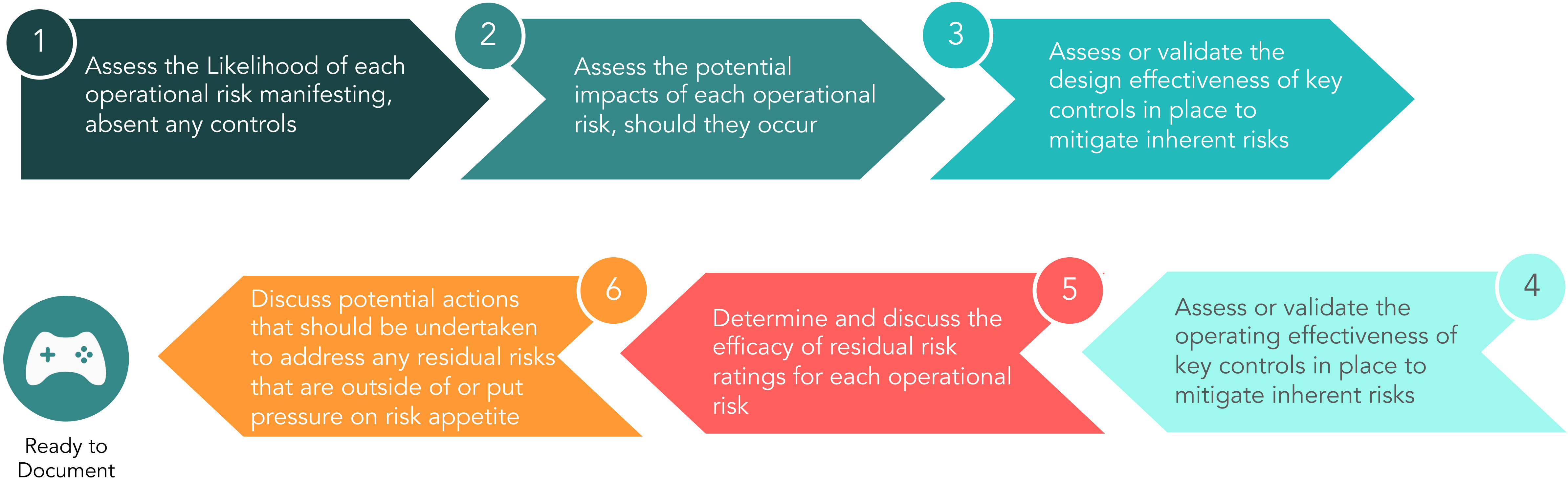
INEFFECTIVE – NEEDS IMPROVEMENT – EFFECTIVE – STRONG

Residual risks above stated risk tolerance must be actioned.

CRITICAL - HIGH – MODERATE – LOW

PHASE 3 – EXECUTE

The key objective of the execute phase is to understand or update your understanding of the AU's operational risk profile



1 Assess the Likelihood of each operational risk manifesting, absent any controls

2 Assess the potential impacts of each operational risk, should they occur

3 Assess or validate the design effectiveness of key controls in place to mitigate inherent risks

4 Assess or validate the operating effectiveness of key controls in place to mitigate inherent risks

5 Determine and discuss the efficacy of residual risk ratings for each operational risk

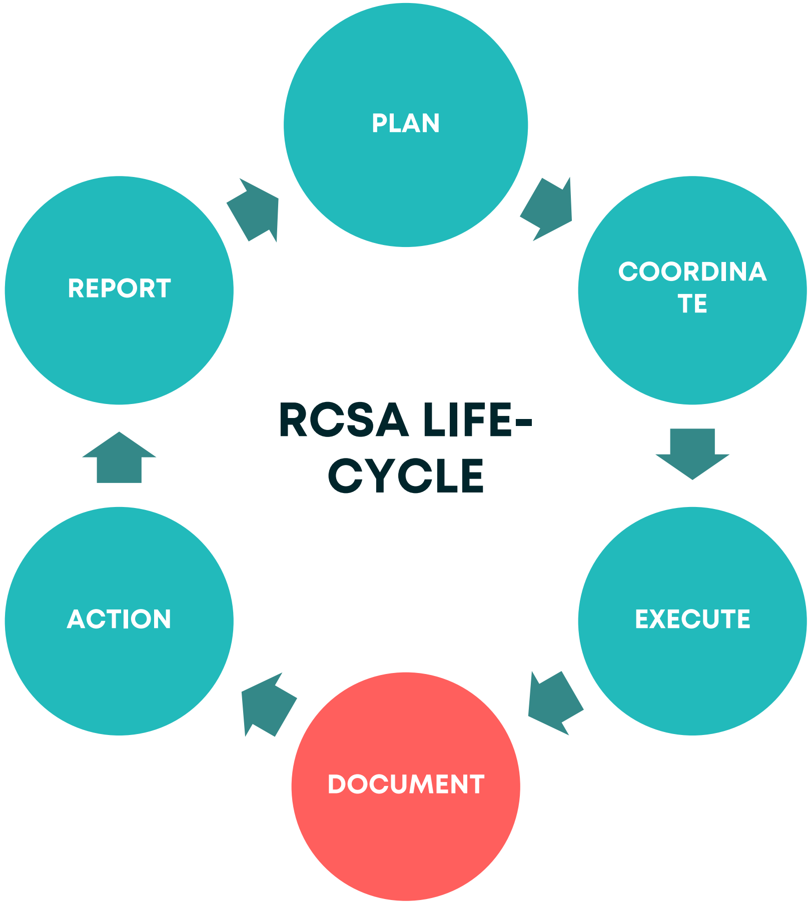
6 Discuss potential actions that should be undertaken to address any residual risks that are outside of or put pressure on risk appetite

Ready to Document

We go into more detail on RCSA execution in Week 3 videos 2 and 3

RCSA LIFE-CYCLE

PHASE 4 – DOCUMENT



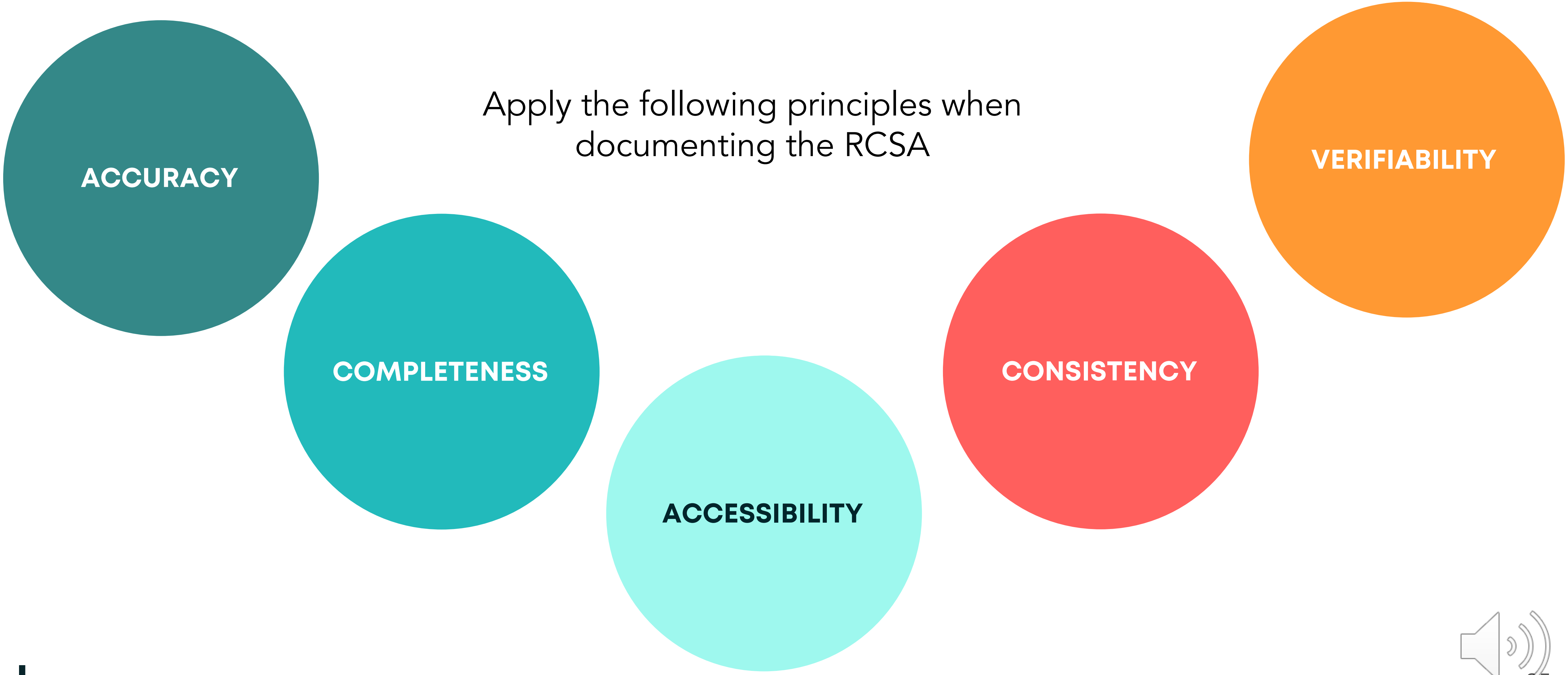
OBJECTIVES

- Support RCSA conclusions with adequate rationale
- Enable effective independent review and challenge and/or auditing
- Demonstrate comprehensive RCSA coverage of the Operational Risk Universe
- Enable consistent aggregation and reporting of RCSA results
- Generate an auditable record of the execution of the RCSA life-cycle
- Act as a source of data for development and implementation of Key Risk and Performance Indicators

PHASE 4 – DOCUMENT

The key objective of the document phase is to ensure there is adequate rationale and evidence supporting conclusions in the RCSA

Apply the following principles when documenting the RCSA


ACCURACY

COMPLETENESS

ACCESSIBILITY

CONSISTENCY

VERIFIABILITY

Illustrative examples of effective rationale supporting conclusions

INHERENT RISK RATING

Processing risk for the AU is rated High, based on the following key driving factors:

- □ Process complexity – high variability of inputs, 40% of steps require judgement, high degree of regulatory scrutiny, and high degree of system interdependence
- □ The AU is handling more than 2.5 million transactions per day, which represents 80% of system capacity
- □ Processing relies on a legacy system, which is already one year past its end-of-life-date

CONTROL EFFECTIVENESS RATING

The Key Control is rated Strong, based on the following factors:

- □ The control is fully documented, preventative, automated, and represents full coverage of the risk;
- □ Testing has been completed in the last 6 months, with no material issues identified;
- □ Individuals performing the control demonstrate the required level of knowledge and skill;
- □ There are no material staffing constraints or vacancies;
- □ No material issues are outstanding; and
- □ Non-material issues have action plans in place and are tracking to plan.

RESIDUAL RISK RATING

Residual Risk is rated Moderate, based on the following key factors:

- □ Inherent Risk is High;
- □ Key Controls are Adequate; and
- □ Outstanding Low Risk issues have action plans in place and are tracking to plan.

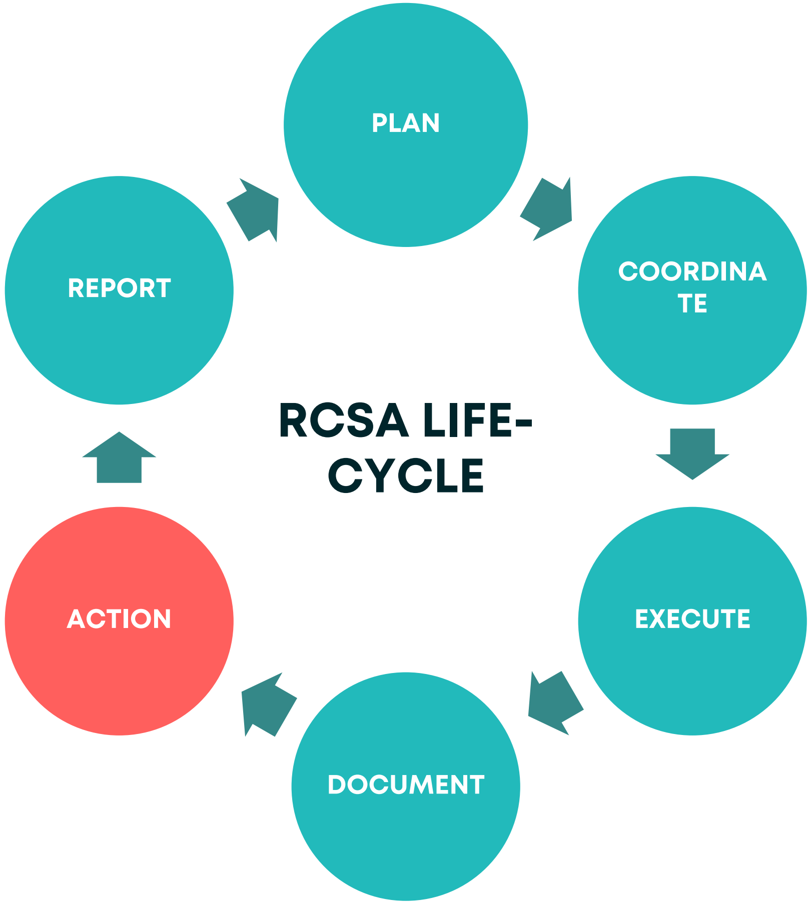
REQUEST FOR OVERRIDE

We are requesting that the auto-calculated Residual Risk Rating be adjusted down from Moderate to Low, based on the following key factors:

- □ The 6 issues driving the downgrade in control effectiveness have not been finalized/confirmed; and
- □ The AU is in process of gathering additional evidence to provide to the Issue Identifier for consideration, prior to finalization of the report (see attached list).

RCSA LIFE-CYCLE

PHASE 5 – ACTION



OBJECTIVES

- Proactively update the Monitoring & Testing Plans to reflect any changes in Operational Risk Profile
- Address any issues identified in the RCSA to avoid operational risk events and to remain within operational risk appetite and tolerance
- Continuously improve the design and operating effectiveness of the ORM program
- Continuously strengthen the firm’s position of operational resilience
- Promote and reinforce First Line accountability for management of Operational Risks

PHASE 4 – ACTION

The key objective of the action phase is to address issues and inform down-stream decision-making and risk-based op risk planning

MONITORING & TESTING – TO-DO

- Update the AU Monitoring Plan
- Update the 2LOD Monitoring Plan
- Update the 2LOD Test Plan
- Update the 1LOD Test Plan

ORM TRAINING – TO-DO

Update the AU's training needs analysis, if needed	AU Owner
Update individual training plans, if needed	AU Owner (or individual's M
Update the ORM Training Plan, if needed	Oversight Fun
Update or enhance the ORM training content, methods, etc if needed	Oversight Fun

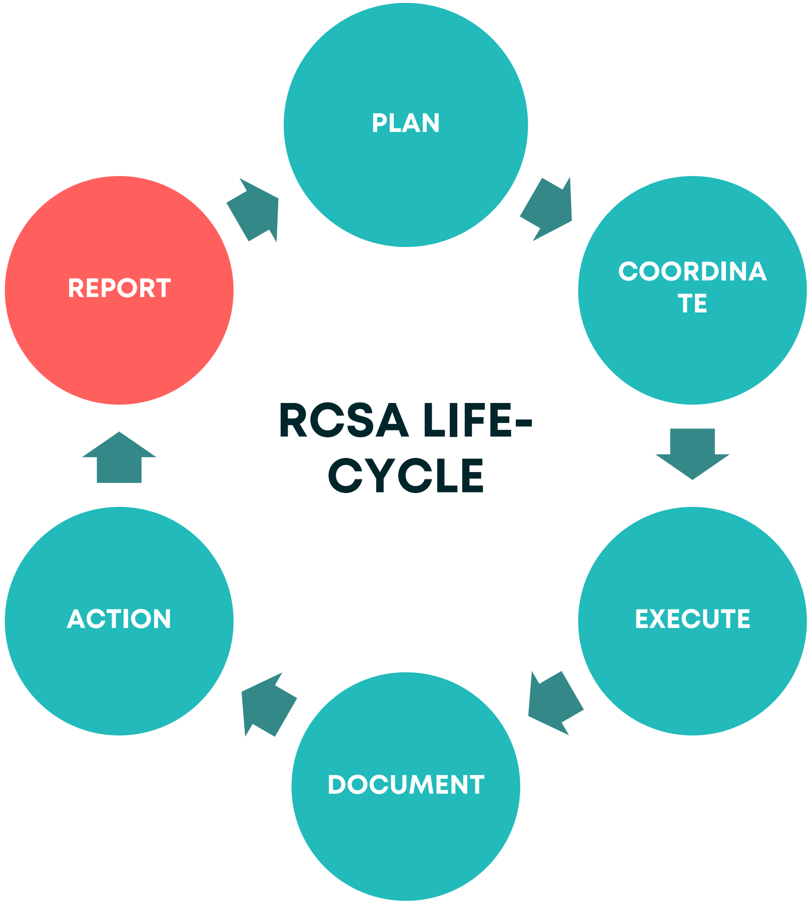
ISSUES MANAGEMENT – TO-DO

Ensure any issues identified during the RCSA are entered into the Issues Repository	AU Owner
Input issues identified during the RCSA into the Issues Repository	Issue Manager(s)
Execute action plans to address any control issues identified during the RCSA	Issue Owner(s)

Issues need to be actioned in accordance with the Issues Management Standards and Procedures

RCSA LIFE-CYCLE

PHASE 6 – REPORT



OBJECTIVES

- Ensure stakeholders are informed about the current operational risk and control environments.
- Ensure decision-makers have the necessary information to make informed decisions regarding operational risk management strategies and resource allocations.
- Promote and reinforce clear accountability for risks and actions to mitigate risks
- Enable prioritization of resources to areas of higher risk

PHASE 6 – REPORT

The key objective of the report phase is to communicate and escalate results of the RCSA to inform strategic decision-making

This is an illustrative example of a typical RCSA Report Table of Contents. For this week's assignment, you'll be asked to innovate and improve upon the status quo.

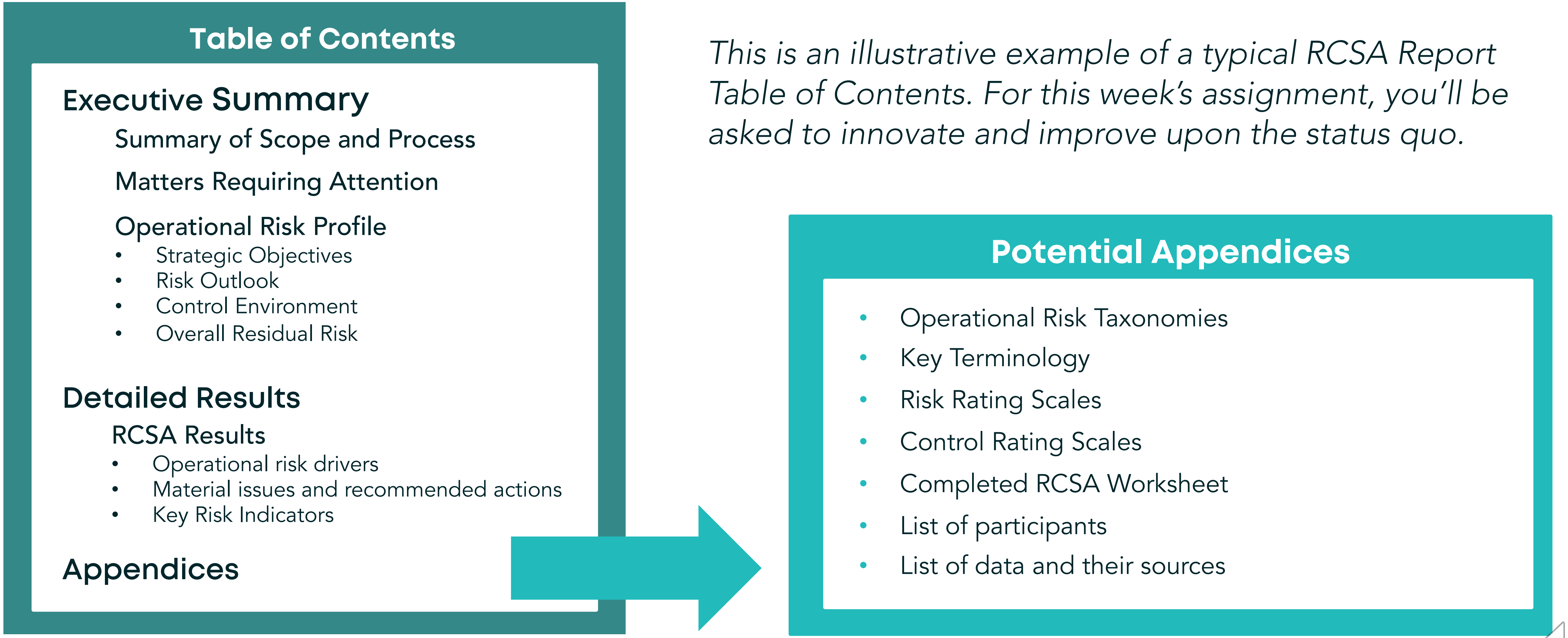


Table of Contents

Executive Summary

Summary of Scope and Process

Matters Requiring Attention

Operational Risk Profile

- Strategic Objectives
- Risk Outlook
- Control Environment
- Overall Residual Risk

Detailed Results

RCSA Results

- Operational risk drivers
- Material issues and recommended actions
- Key Risk Indicators

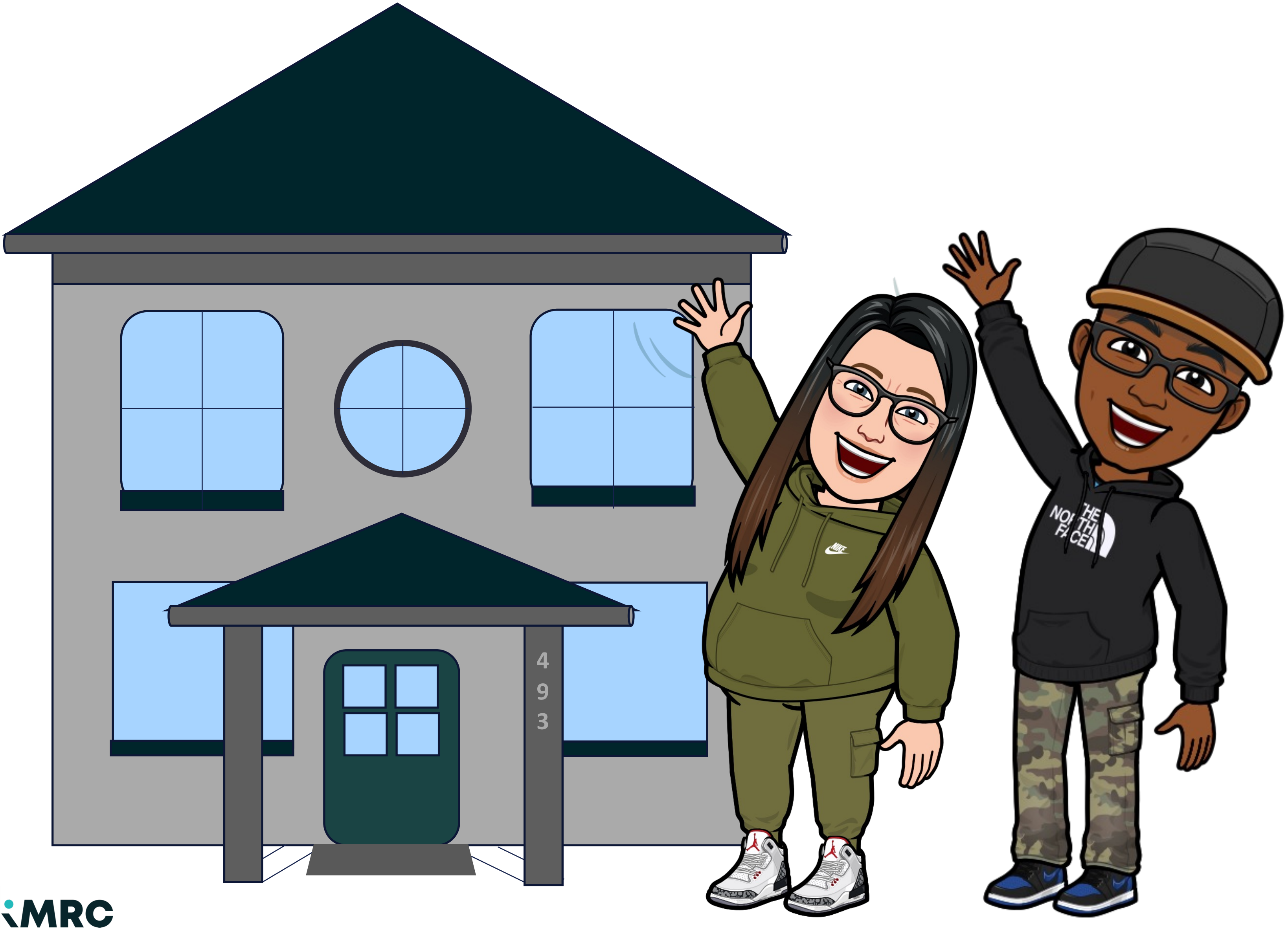
Appendices

Potential Appendices

- Operational Risk Taxonomies
- Key Terminology
- Risk Rating Scales
- Control Rating Scales
- Completed RCSA Worksheet
- List of participants
- List of data and their sources

RCSA EXERCISE

WELCOME TO THE MILLER HOME!



SCENARIO

The Millers have recently purchased their dream home in a sought after gated community.

The home is a single-detached house in a condominium community that includes the following shared common spaces:

- Pool
- Gym
- Golf course
- Tennis courts
- Club house

Part of the appeal of the condo community is that part of their condo fees will go towards home maintenance. This is the first condominium community that the Millers have ever lived in and they want to make sure they manage their operational risks to maximize their happiness.

Can you help the Millers to perform an assessment of the operational risks at their new home?

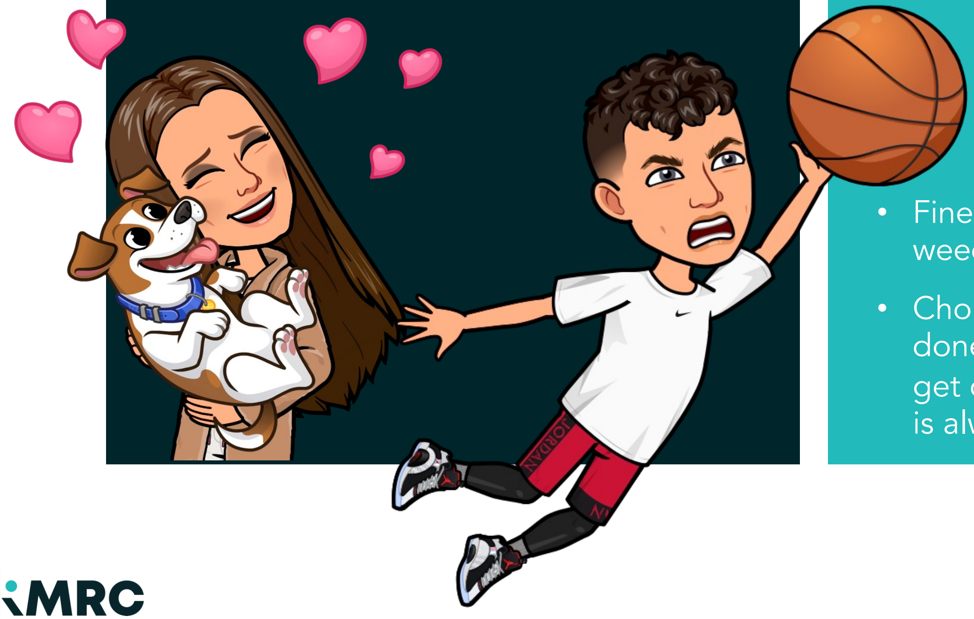
INHERENT RISK ASSESSMENT

FAMILY PROFILE

Given the Family Profile, what AU profile rating do you think is appropriate? High Risk, Moderate Risk, or Low Risk? For purposes of our assignment, let's just apply judgement:

ABOUT THE FAMILY

The Millers live with their two children, Nick (age 12), Dot (age 16) and their dog Liam. They are a busy family who are always on the go. Their home is the place where friends and family gather.



HISTORY OF ISSUES

At their last home, they fell behind on home maintenance during the pandemic, which resulted in a few material events:

- Leaks in roof caused by replacement of shingles that were not properly sealed that that ended up spilling into the kitchen
    - Basement flood caused by inadequately positioned downspouts (some spots on the house were missing after a terrible summer storm)
- Fined by city for failing to keep weeds and growth under control
- Chores have been challenging to get done with their busy schedule – tasks get done last minute or late. Quality is always disputed.

USES AND OCCUPANCY

4 months out of the year, Mrs. Miller's parents, who live outside of country, stay with them. They have a dog and a cat.

Mr. Miller is an attorney who runs a private practice out of his home.

Ms. Miller is a risk consultant and commutes to client offices 2 days a week. The other three days, she works from home.

Mrs. Miller is an avid volunteer for many organizations and often hosts meetings and events at home. Part of the appeal of the condominium community was the Club House, which includes much more functional space for these purposes.