Risk and Control Self-Assessment (RCSA)

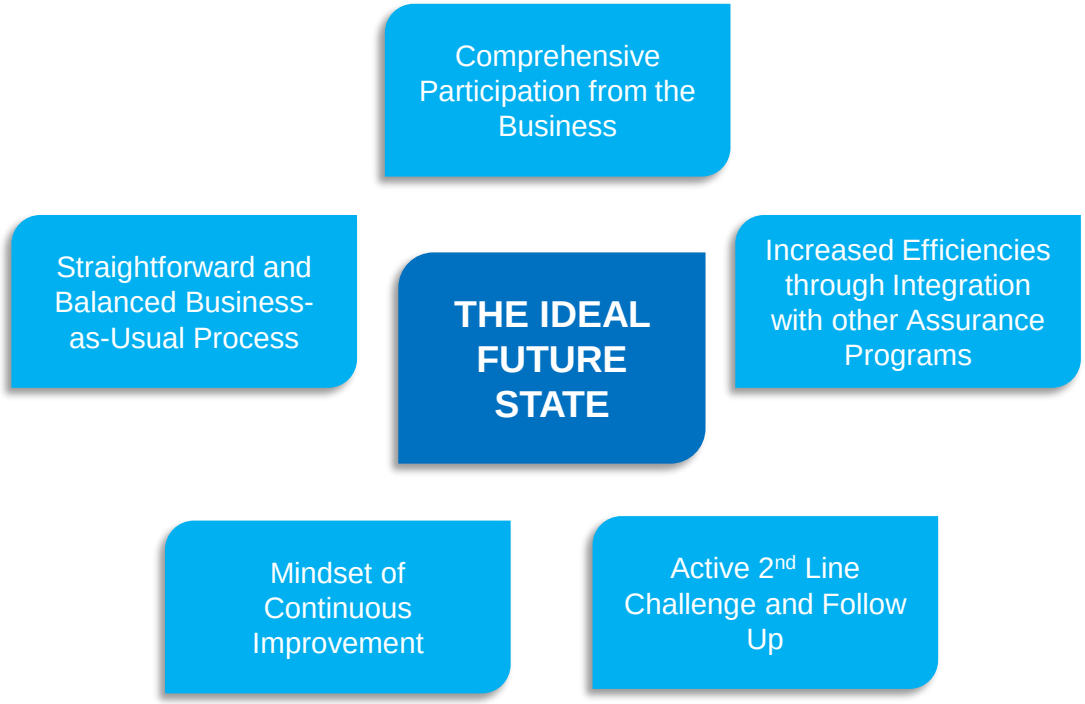
Overview and Discussion Document for Internal Audit Group (IAG)
July 2018

RCSA Program and Transformation Overview

Overview

The Risk and Control Self-Assessment (RCSA) is a process that organizations employ to analyze their control environment in order to inform specific business or legal entity operational risk profiles. Unlike other assurance review processes such as internal audit and second line independent reviews, the RCSA is a business-owned activity. The primary benefits of the RCSA include:

- Continuous and dynamic analysis of operational risk profiles by logical business units.
- Strengthen and help optimize control environments.
- Help promote an integrated and holistic views of risk.
- Reinforce risk culture in the business.
- Reducing audit fatigue and efforts required for audit testing of controls.



RCSA Clarified: Official Definition

A Risk and Control Self-Assessment (RCSA) is a business practice that helps first line risk owners identify and appraise significant risks inherent in the business operations. An RCSA program and its process also helps management with evaluating the effectiveness of controls and reduce the potential for operational losses through proactive risk treatment options. The RCSA process promotes first line risk accountability and awareness by incorporating risk management practices into the regular course of business operations.

RCSA Transformation

AIG's Risk and Control Self-Assessment (RCSA) program has undergone multiple iterations of enhancements over the past several years resulting in diluted value of the RCSA to the business in terms of managing control environments and ability to perform business unit risk profiling. The desired benefits from RCSAs have also suffered from inconsistent use of taxonomies (e.g. PRC) across business units and functions, complex process and IT enabler. The need for simplification is warranted to ensure that expected benefits are achieved, first-line can ultimately own the process, and ERM can provide more effective review and challenge.

	Challenges Addressed	Outcomes
Coverage Model	▪ Undefined assessment universe, thus resulting in gaps in coverage and inability to aggregate RCSA results. ▪ Inconsistent and incomplete coverage of processes and risks. ▪ Second line driven prioritization and execution of RCSAs.	▪ Defined the level of assessment expected (Org L4) and maintenance of an assessment universe (WIP) ▪ Requirement for end-to-end coverage in RCSAs (e.g. all applicable processes).
Assessment Methodology	▪ Methodology for risk and control identification, and assessment were driven by the need to address Fed observations, resulting in a program exceeding AIG's maturity.	▪ RCSA assessment life-cycle requirements and workflow have been streamlined, and simplified while retaining comprehensive risk considerations. ▪ Control evaluation simplified with increased focus on operating effectiveness.
Common Taxonomies	▪ Evolving PRC and inconsistent use have impacted the consistency in assessments, and the ability to aggregate and report results has been practically impossible	▪ PRC streamlined in Q1 2018 (overall 60% reduction in PRC records) to be used as authoritative source for risk and control identification during RCSA.
System and Tools	▪ The current system of record, Archer, lacks functionality to meet management desire and suffers from complexities making it an unsuitable solution for use by the 1st line.	▪ Created initial vision, prototype, and requirements for intuitive fit to purpose IT solution / enabler for first line to execute RCSA and better manage issues and actions tied to assessments.

AIG

RCSA Accountability Model

RCSA Definition	RCSA Standard	1st Line Responsibility TAKE & MANAGE RISK	2nd Line Responsibility SET RISK POLICY, MONITOR & CHALLENGE	3rd Line Responsibility VALIDATE & TEST
A Risk and Control Self-Assessment (RCSA) is a business practice that helps first line risk owners identify and appraise significant risks inherent in the business operations. An RCSA program and its process also helps management with evaluating the effectiveness of controls and reduce the potential for operational losses through proactive risk treatment options. The RCSA process promotes first line risk accountability and awareness by incorporating risk management practices into the regular course of business operations.	The RCSA standard is been updated and calls for RCSAs to be performed annually at the appropriate level of the organizational hierarchy, at a minimum of the level four of the organizational hierarchy x product x geography. **Example:** AIG>GI>Specialty>Marine x Geography (Marine US)	Line of business managers are responsible for the execution of the RCSA process. This encompasses: • process selection, • identification of risks and inherent risk assessment, • control evaluation, • residual risk rating, and • risk treatment - identifying issues, action plans and potential risk acceptances.	ERMs role in the RCSA process is to: • enforce RCSA requirements, • perform effective review and challenge, and • provide for active risk oversight and insights & analytics. • facilitate training of tools and processes to ensure understanding by business managers executing RCSAs.	IAG will evaluate the design and operating effectiveness of the RCSA implemented by the business as well as ERM's review and challenge process.
		Expected Benefits		
		• Comprehensive annual risk assessment coverage; • Increase in self-identified issues; • Reduction of potential operational losses; • Identification of pervasive/thematic risks/issues.	• Strengthen risk oversight capabilities and focus on independent risk reviews (e.g., Deep Dives); • Focus on RCSA review and challenge; • Provide for enhanced monitoring and aggregate risk analytics and insights.	• RCSA results used for Audit Planning; • Assessment of management's risk culture and awareness.

RCSA Workflow – Future State

The streamlining of the RCSA process focuses on simplifying the workflow of a typical RCSA, and the requirements for inputs in each step.

FUTURE STATE RCSA WORKFLOW

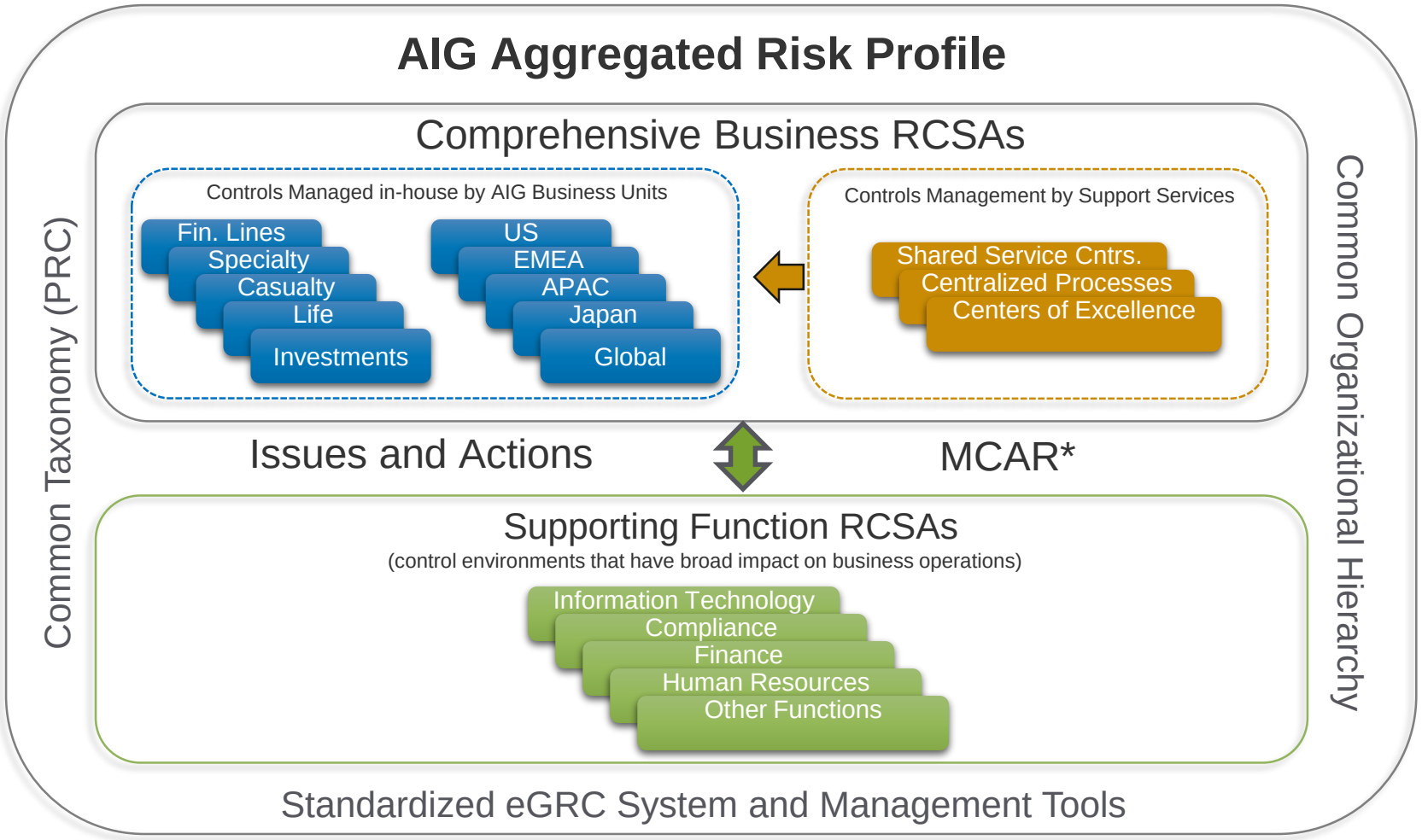
Streamlined and Simplified Workflow, PRC, and Assessment Input Requirements

Simplified Issues Management Process

Enhanced Risk-Based Second Line Challenge

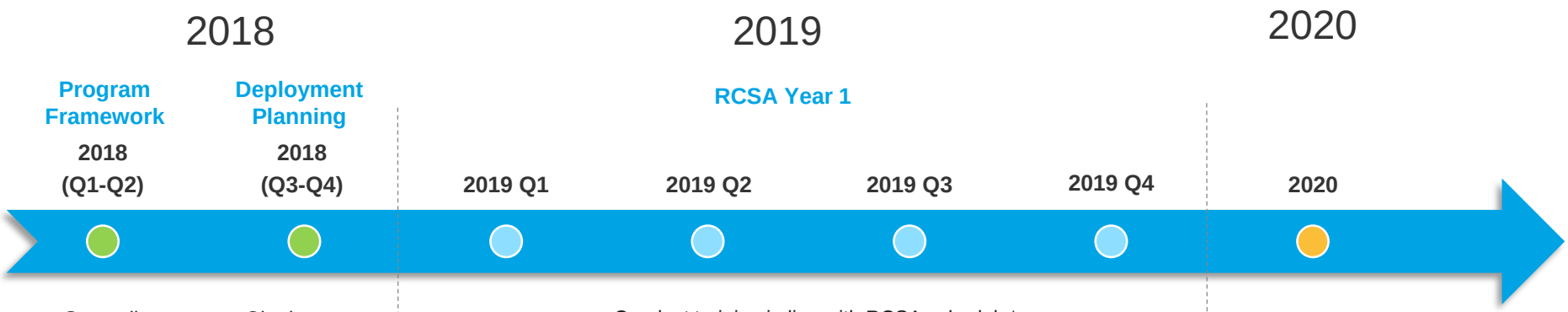
A simpler data model that enablers better insights to operational risk

The future state RCSA will provide insights and holistic views of risk across AIG through comprehensive assessments and linkage between the various control environment elements that make up the risk profile of any given business unit.



*MCAR is IAG's proposed Management Control Awareness Rating.

Timeline of Activities (Proposed)



- Streamline methodology and develop IT enabler requirements.
- Develop comprehensive assessment universe / coverage model.
- Develop governance and engagement model.

- Obtain leadership sponsorship.
- Agree with business units and develop deployment plans in tranches (logical units/regions).
- Build / customize IT enabler.
- Complete PRC Reviews.
- Develop training program.
- Finalize 2019 prioritized RCSA schedule.

- Conduct training in line with RCSA schedule*.
- Q1 RCSAs Commence
- Q2 RCSAs Commence
- Q3RCSAs Commence
- Q4 RCSAs Commence
- Second line dedicated guidance for year 1 RCSAs
- Ongoing monitoring of progress and program effectiveness.
- Prioritization of 2020 RCSAs
- Barometer check on effectiveness of program through the lens of success criteria, including expected increase in self-identified issues.
- Develop analytics / year 1 report.

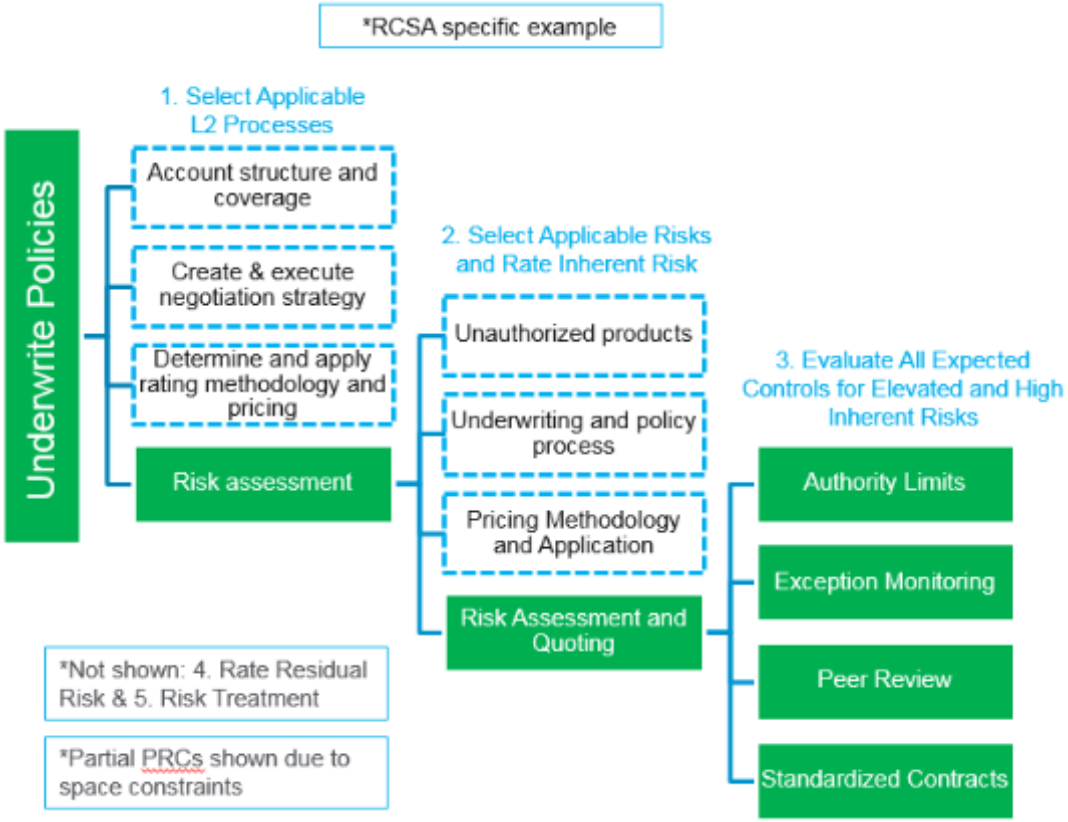
* Some training may be conducted in 2018 based on RCSA schedule.

- 2020 RCSAs Commence.
- Develop plan to shift RCSA to BAU for 2021+

Performing an RCSA

Before we Start……Use of the PRC

- **Consistent Input Mechanism for Risk Programs**
  - The PRC serves as a consistent input mechanism for risk programs (Risk Events, Issues and Actions Management, RCSA), supporting completeness and accuracy of data. In the past these programs were not unified by a consistent method of input, creating data inconsistencies.
- **Usage During an Operational Risk Assessment**
  - The PRC supports the completeness of risks and controls considered during assessment and consistency in execution of assessments.



1. Pre-Work

Prior to starting the RCSA, it is essential that Management understand the process flow and procedures, systems, handoff areas, and have a strong understanding of the business/function profile. This step also allows for:

- Understanding areas that pose higher risk
- Correlation with other programs to avoid unnecessary work (e.g. control already found to be ineffective), and avoiding contradictory results.

The information reviewed as part of pre-work can include:

Top Risks (includes AIG Enterprise, Business Unit, and Function Top Risks)	Key Risk Indicators ("KRIs")
Business strategy plans and quarterly business reviews	External Reports (Auditor, Consultants)
Financial Data	Regulatory Findings
Headcount	Assessments of other line functions) (e.g. Audit, TRO, Compliance, SOX,)
Organizational Structure/Hierarchy	Process Policies and Procedures and/or desktop manuals
Emerging Risk	Process Maps (new, transformation, SOX)
Internal and External Risk Events Capture and Reporting	

2. Select Processes, Identify Risks

(RCSA Standard) Processes are activities undertaken to achieve objectives of a business or function. Unless an RCSA has been pre-defined as targeted, all processes applicable to a business or function undergoing RCSA should be assessed with the **objective of attaining an end-to-end view of the risk and control environment**. The appropriate subject matter experts (SMEs) (e.g. process and control owners) should be engaged during an RCSA to ensure that processes are assessed and documented.

Purpose:

- Define the scope for the RCSA and areas to be assessed.

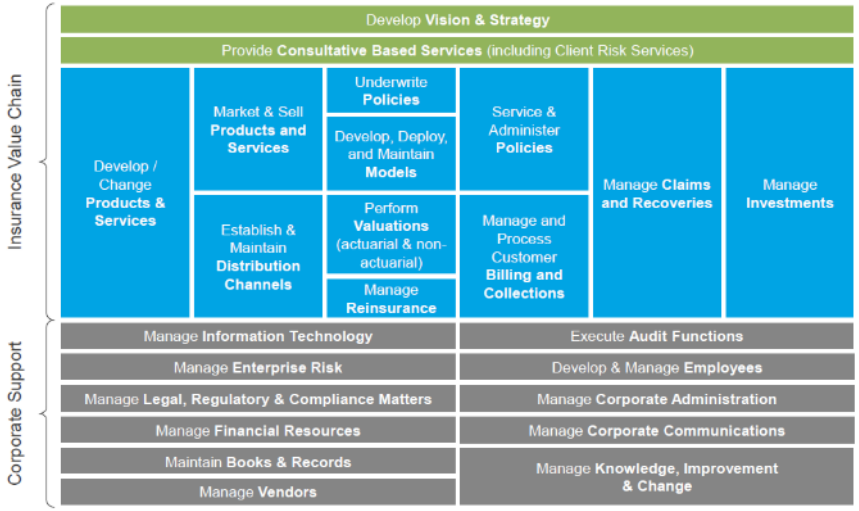
Select Processes:

- RCSAs are expected to be end-to-end.
- All applicable processes from the taxonomy are selected.

Identify Risks:

- The PRC contains risk to process linkages.
- All risks that come with a process are selected.

Process Taxonomy



PRC Risks

Process		Risk		
Level 1 Process Name	Business Process Level 2	Risk Unique ID	Risk Level 3	Risk Level 3 Description
Underwrite Policies	Account structure and coverage	RSK3-1162	Account Structure and Coverage:	Account structure, price and/or risk exposure determination is incorrect.
		RSK3-1215	Client Services Accounts:	New or existing account set up is incorrect or overly complex in coverage.
		RSK3-1180	Unauthorized products:	Risk associated with unauthorized insurance products being offered for sale.
	Create & execute negotiation strategy	RSK3-1055	Risk Assessment and Quoting:	Policy quotes are inaccurate and/or unacceptable levels of risk are quoted.

Notes:

- Some processes (fully or partially) for a given assessment unit may be managed by another group (e.g. shared service).
- The supporting groups will perform RCSAs on those processes. Results will subsequently be incorporated.

3. Assess Inherent Risk Materiality

(RCSA Standard) The primary purpose of assessing inherent risk is to **determine, or identify, those risks that should receive the highest level of focus** for control evaluation and prioritization. **Higher inherent risks generally pose greater threat to the organization** should the risk materialize and, therefore, **require a stricter level of controls and monitoring** of the effectiveness of controls.

Purpose:

- Prioritize the most significant risks for control evaluation.
- Elevated and High inherent risks required control evaluation at a minimum.

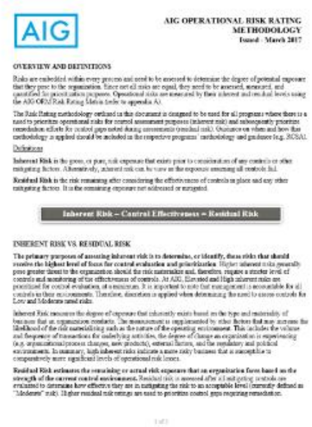
Rate Inherent Risks:

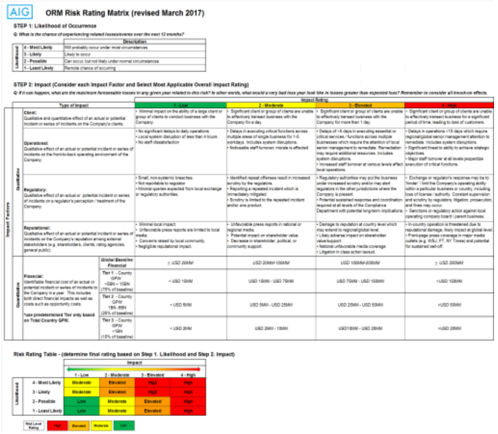
- Each risk is rated using a simplified inherent risk rating approach.
- The AIG Operational Risk Rating Methodology is leveraged

Justify Decisions:

- Rationale are required for ratings with focus on risks deemed Low/Moderate.
- Risks deemed “Not Applicable” must be justified.

AIG Operational Risk Rating Methodology





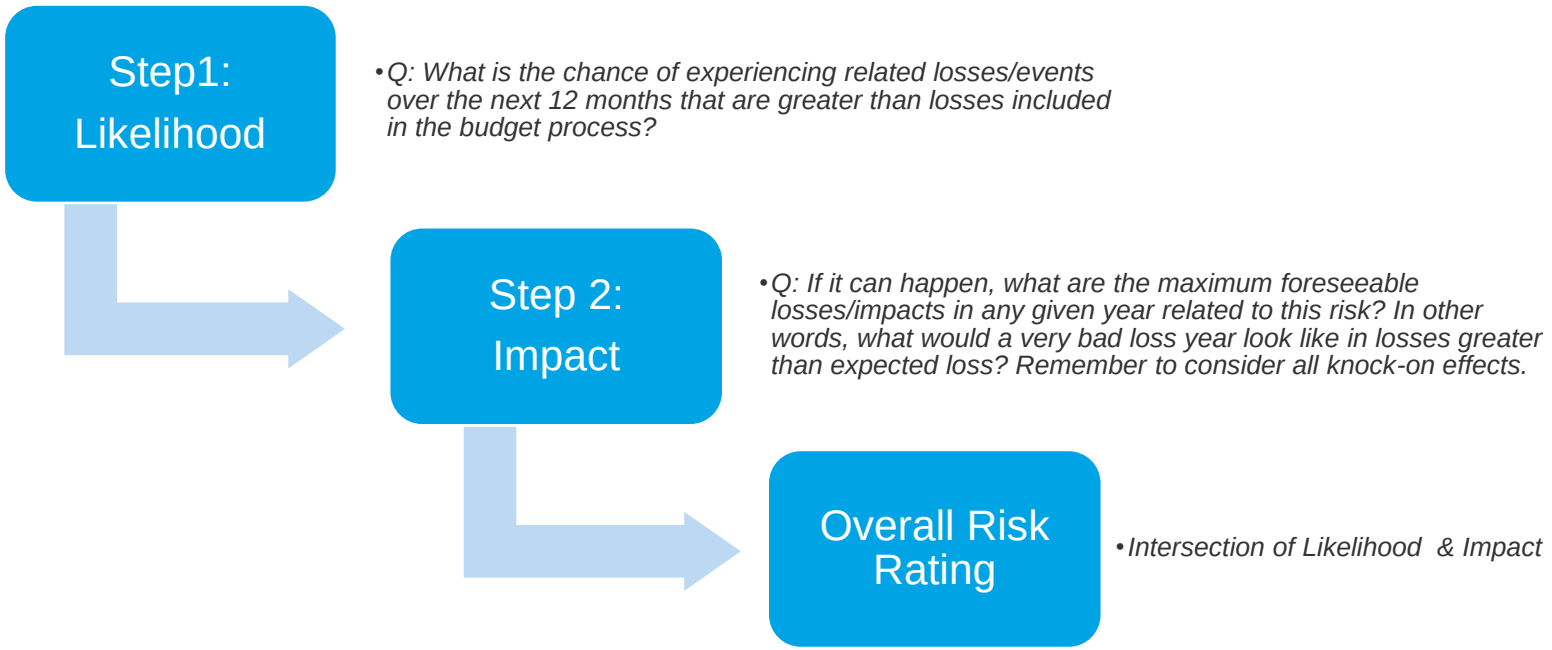
Inherent Risk Assessment

Risk					
		RCSA Inherent Risk Assessment			
Risk Level 3	Risk Level 3 Description	Business Risk Description	Inherent Risk Rating	Inherent Risk Rating Rationale
Channel Strategy and Distribution:	Product offerings do not reach intended markets effectively and/or are misunderstood or misinterpreted.	*Text*	Elevated	*Text*

3. Assess Inherent Risk Materiality, cont'd

Inherent Risk is the gross, or pure, risk exposure that exists prior to consideration of any controls or other mitigating factors. Alternatively, inherent risk can be viewed as the exposure assuming all controls fail. Higher inherent risks generally pose greater threat to the organization should the risk materialize and, therefore, require a stricter level of controls and monitoring of the effectiveness of controls.

The ORM Risk Rating Matrix is used to perform an inherent risk assessment via a step process; (1) likelihood of a risk occurring and (2) the potential impact/losses that could be incurred. Impacts are determined taking in both qualitative and quantitative factors.



ORM Risk Rating Matrix (revised March 2017)

STEP 1: Likelihood of Occurrence

Q: What is the chance of experiencing related losses/events over the next 12 months?

		Description
Likelihood	**4 - Most Likely**	Will probably occur under most circumstances
	3 - Likely	Likely to occur
	2 - Possible	Can occur, but not likely under normal circumstances
	1 - Least Likely	Remote chance of occurring

STEP 2: Impact (Consider each Impact Factor and Select Most Applicable Overall Impact Rating)

Q: If it can happen, what are the maximum foreseeable losses in any given year related to this risk? In other words, what would a very bad loss year look like in losses greater than expected loss? Remember to consider all knock-on effects.

Impact Factors		Type of Impact		Impact Rating: 1 - Low	2 - Moderate	3 - Elevated	4 - High
	Qualitative	**Client:** Qualitative and quantitative effect of an actual or potential incident or series of incidents on the Company's clients.		• Minimal impact on the ability of a large client or group of clients to conduct business with the Company.	• Significant client or group of clients are unable to effectively transact business with the Company for a day.	• Significant client or group of clients are unable to effectively transact business with the Company for more than 1 day.	• Significant client or group of clients are unable to effectively transact business for a significant period of time, leading to loss of customers.
		Operational: Qualitative effect of an actual or potential incident or series of incidents on the front-to-back operating environment of the Company.		• No significant delays to daily operations • Local system disruption of less than 4 hours • No staff dissatisfaction	• Delays in executing critical functions across multiple areas of single business for 1-5 workdays. Includes system disruptions. • Noticeable staff turnover; morale is affected	• Delays of >5 days in executing essential or critical services / functions across multiple businesses which require the attention of local senior management to remediate. Remediation may require additional resources. Includes system disruptions. • Increased staff turnover at various levels affect local operations.	• Delays in operations >10 days which require regional/global senior management attention to remediate. Includes system disruptions. • Significant threat to ability to achieve strategic objectives. • Major staff turnover at all levels jeopardize execution of critical functions.
		Regulatory: Qualitative effect of an actual or potential incident or series of incidents on a regulator's perception / treatment of the Company.		• Small, non-systemic breaches. • Not reportable to regulator • Minimal queries expected from local exchange or regulatory authorities.	• Identified repeat offenses result in increased scrutiny by the regulators. • Reporting a repeated incident which is immediately mitigated • Scrutiny is limited to the repeated incident and/or one product.	• Regulatory authorities may put the business under increased scrutiny and/or may alert regulators in the other jurisdictions where the Company is present. • Potential sustained response and coordination required at all levels of the Compliance Department with potential long-term implications.	• Exchange or regulator's response may be to 'hinder' / limit the Company's operating ability within a particular business or country, including loss of license / authority. Constant supervision and scrutiny by regulators; litigation, prosecution, and fines may occur. • Sanctions or regulatory action against local operating company board / parent business.
		Reputational: Qualitative effect of an actual or potential incident or series of incidents on the Company's reputation among external stakeholders (e.g. shareholders, clients, rating agencies, general public).		• Minimal local impact. • Unfavorable press reports are limited to local media. • Concerns raised by local community. • Negligible reputational impact.	• Unfavorable press reports in national or regional media. • Potential impact on shareholder value. • Decrease in shareholder, political, or community support.	• Damage to reputation at country level which may extend to regional/global level. • Likely adverse impact on shareholder value/support. • National unfavorable media coverage • Litigation in class action lawsuit.	• In-country operation is threatened due to reputational damage, likely impact at global level. • Front-page press coverage in major media outlets (e.g. WSJ, FT, NY Times) and potential for sustained sell-off.
	Quantitative	**Financial:** Identifiable financial cost of an actual or potential incident or series of incidents to the Company in a year. This includes both direct financial impacts as well as costs such as opportunity costs. ***use predetermined Tier only based on Total Country GPW.**	***Global Baseline Financial***	*≤ USD 20MM*	*USD 20MM-100MM*	*USD 100MM-200MM*	*≥ USD 200MM*
			Tier 1 - Country GPW >5BN – 15BN (75% of baseline)	< USD 15MM	USD 15MM - USD 75MM	USD 75MM - USD 150MM	>USD 150MM
			Tier 2 - Country GPW 1BN -5BN (25% of baseline)	< USD 5MM	USD 5MM - USD 25MM	USD 25MM - USD 50MM	>USD 50MM
			Tier 3 - Country GPW <1BN (10% of baseline)	< USD 2MM	USD 2MM - 10MM	USD10MM - USD 20MM	>USD 20MM

Risk Rating Table - (determine final rating based on Step 1. Likelihood and Step 2. Impact)

		Impact: 1 - Low	2 - Moderate	3 - Elevated	4 - High
Likelihood	**4 - Most Likely**	Moderate	Elevated	High	High
	3 - Likely	Moderate	Elevated	High	High
	2 - Possible	Low	Moderate	Elevated	High
	1 - Least Likely	Low	Moderate	Elevated	High

Risk Level Rating	High	Elevated	Moderate	Low

3. Assess Inherent Risk Materiality, cont'd

Supplemental Guidance and Definitions in Draft Revised RCSA Standard

Inherent Risk Rating	Description *If controls are not in place, or all controls fail:*	Requires Control Evaluation in RCSA?
High	Risks that could result in unacceptable losses and/or have the most significant impact on achieving strategic and or business objectives should they occur. A High rating takes into account risks that have a high chance of occurring in the absence of controls with a high impact (single event or aggregate of events), as well as those with a low chance of occurring, but with significant impact should they occur. The effectiveness of the control environment for mitigating High inherent risks is a top priority.	**Yes**
Elevated	A secondary tier of material risks when considering the chance of occurrence and impact. While not as critical as High risks, Elevated risks could still result in impacts or losses unacceptable to Management should they occur, and warrant careful monitoring of the control environment.	**Yes**
Moderate	Risk deemed acceptable by Management in the regular course of business. Management should apply their knowledge of the risk environment and discretion in determining whether to perform control evaluations for these risks. If a moderate risk is deemed significant enough to require control evaluation then it is recommended that the inherent risk rating be revisited to determine if the risk should potentially be rated higher.	**Management Discretion**
Low	Risks that are of minimal concern to Management, and could be easily rectified should they occur with little to no impact.	**Management Discretion**

3. Assess Inherent Risk Materiality, cont'd

Example RCSA - Aerospace US	Tier 1 Financial Factor (in matrix based on US GPW)
Risk: Risk associated with breach of underwriting authorities, guidelines, limits, referral or approved appetite by inexperienced underwriter(s), administrator(s) or agent(s) leading to increased exposure to loss, adverse claims experience or acceptance of unquantified risk exposures and/or unprofitable business.	

Step 1: Likelihood

Q: What is the chance of experiencing losses/events related to U/W breaches over the next 12 months that are greater than losses included in the budget process?

Answer: 4 - Most Likely

Why? :

A significant number of prior events are known as well as previous years' RCSA findings.

This is a top risk for Commercial

U/W is a core process with high volumes of related transactions increasing the risk that events occur.

Supporting infrastructure/systems are outdated with manual workarounds prone to error/circumvention of u/w guidelines.

Step 2: Impact

Q: If it can happen, what are the maximum foreseeable losses/impacts in any given year related to this risk? In other words, what would a very bad loss year look like in losses greater than expected loss? Remember to consider all knock-on effects.

Answer: 250mm ("High" >150mm per matrix)

Why?

This is based on the volume and dollars amounts of policies that could be impacted. Significant knock-on effect would be incorrect reinsurance placements.

Note: some RCSAs will opt to use a qualitative factor (e.g. regulators may fine us… resulting in reputational damage… resulting in lost opportunities for new businesses….)

Risk Rating Table - (determine final rating based on Step 1. Likelihood and Step 2. Impact)

Likelihood	Impact: 1 - Low	2 - Moderate	3 - Elevated	4 - High
4 - Most Likely	Moderate	Elevated	High	High
3 - Likely	Moderate	Elevated	High	High
2 - Possible	Low	Moderate	Elevated	High
1 - Least Likely	Low	Moderate	Elevated	High

Risk Level Rating	High	Elevated	Moderate	Low

4. Identify and Evaluate Controls

(RCSA Standard) Controls are activities designed to **provide reasonable (not 100%) mitigation of risks**: achievement of objectives relating to business operations, reporting, and compliance with internal policies, procedures and external regulations. **Properly designed and functioning controls** are integral to mitigating inherent risks in the business. It is the responsibility of Management to ensure that the **control objectives are identified, assessed, and documented** within the RCSA

Purpose:

- Identify and evaluate the effectiveness of ”expected” controls mitigating operational risks.
- Identify gaps requiring management action.

Identify “Expected” Controls:

- Expected controls are those that management deems necessary to adequately mitigate a risk given the potential failure points.
- Consideration is given to the right level of controls required (e.g. avoid over-controlling).

Evaluate “Expected” Controls:

- Both Design and Operating Effectiveness are considered.
- An overall rating is selected.
- A rationale as to how Management gained comfort that each controls is actually working is required.

Design Considerations

Design Factors	
Repeatable	Is the control designed in a way that allows it to be repeatable over time?
Frequency	Does the control operate at a scheduled frequency that supports the process/risk?
Automation	Does the level of automation support the complexity of the process/data?
Operation	Does the control owner have sufficient knowledge of the control procedures or is the control functioning as intended?
Known Factors	Do prior Audits, Loss Events, KRIs or RCSA results indicate a design or operating flaw?
Exceptions	Are the exceptions or control failures apparent from the output of the control?
Exception Follow Through	Does the control provide examination, review or resolution of exceptions identified?
Evidence	Can the operation of the control be easily demonstrated, documented and understood by a 3rd party?

Operation Considerations

Operation Method / Indicators	
Observation	Perform a walkthrough of the control in action. Is the process/control being performed as described or intended?
Risk Metrics (KRIs/KPIs)	If the business has KRIs/KPIs that produce metrics related to the controls being evaluated do they adequately measure the control? Do they cover all key elements and inputs from a completeness perspective? Do they capture the essence of the underlying risk?
Issues (Loss Events, Audit Findings)	Have the control gaps identified during prior issues been resolved (action plan closure)? Is the process/control being managed today based on the control enhancements or improvements following the action plan closure?
Sample/Artifact Substantiation	Do control documents/reports or other artifacts evidence the control is being properly executed based on the required frequency, scope, and design?
Recurring or Known Issues (Issues, Risk, Acceptances)	Are there recurring issues or events that suggest that the control continues to fail? If a control is ineffective and not operational, when will it be remediated in order for re-evaluation?

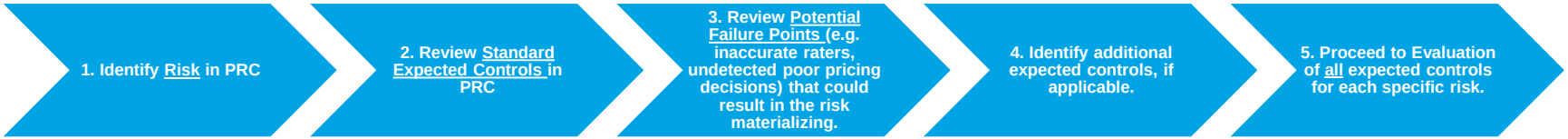
Control Evaluation

Risk		Control			RCSA Control Evaluation		
Risk Level 3	Risk Level 3 Description	Control ID	Control Name	Control Description	Business Control Description	Control Effectiveness Rating	Rating Rationale
Claims: Disbursements:	Disbursements are inaccurate or unauthorized.	CTRL-1477	Automated, rule-based transaction filtering	Automated preventive control filtering or preventing transactions from being executed that do not meet	Text	Partially Effective	Text
		CTRL-1090	Documentation Legitimacy Monitoring, Review and Escalation	Guidelines require that specific claim documentation is submitted (i.e., proof of loss) timely upon receipt of claim. The claim documentation must be reviewed for legitimacy and approved before recovery payments are processed. Additional claims that exceed certain thresholds must receive additional	Text	Effective	Text
		CTRL-1021	Exception Monitoring	Exceptions are properly identified, researched, escalated and resolved in a timely and appropriate manner. Processes exits to monitor the status and resolution of exceptions in accordance with policy and procedures	Text	Ineffective	Text
		CTRL-1472	Peer Review / Quality Control	Second pair of eyes review to check the substantive quality, accuracy or completeness of transactions or business actions.	Text	Effective	Text
		CTRL-1470	Segregation of Duties	Job-enforced or system-enforced separation of non-compatible activities to prevent a single person from executing unauthorized transactions. Typical segregations include: custody and recording, input and approval, etc.	Text	Effective	Text
		CTRL-1549	Verification of Settlement Instructions	Standard settlement instructions and related modifications are reviewed and approved.	Text	Effective	Text

4. Identify and Evaluate Controls, cont'd

- To adequately mitigate a risk, a group of "expected" controls work together to mitigate the risk.
- Standard expected controls are linked to each risk in the PRC.
- **Each standard expected control in the PRC must be evaluated. If a control is not applicable, then should be noted as such in Archer with a rationale.**
- Standard expected controls are typically generic enough to allow for flexibility in mapping business specific controls.

Control Evaluation Steps



Control Ratings

Control Effectiveness Rating	Description
Effective	• Control is well established, relevant and deemed reliable in mitigating the risk of loss • The control is appropriately designed and executed as intended
Partially Effective	• There is only partial fulfilment or adherence, and risk mitigation with the control as stated (i.e. the control is not being performed with full effectiveness, is being performed inconsistently or with irregular frequency) • Control design needs some improvement (may not be fully effective in mitigating risk), or the design might be manual (where automated controls would be more effective)

Ineffective	• Control does not mitigate the risk that is inherent in the key business process:
	  • The control either does not exist or, if in place does not mitigate the portion of the risk for which it is designed (the control design is inadequate in mitigating the risk and requires significant redesign),or
	  • The control is performed improperly or not at all

Not Applicable	• The control has not been deemed as an "expected" controls or does not apply to the environment undergoing assessment. A detailed rationale is required to justify any control deemed N/A.

5. Assess Residual Risks

(RCSA Standard) After documenting controls for each risk and determining their effectiveness, Management will rate each risk from a Residual risk perspective. Residual risk takes into account the same likelihood and impact concepts outlined for inherent risk above with one major difference; the effectiveness of the group of expected controls now influences the rating. In other words, the **remaining risk after controls is determined**.

Purpose:

- For each risk, determine whether remaining risk exposure is within tolerance after the effectiveness of controls is evaluated.
- Use the results to determine risk treatments needed.

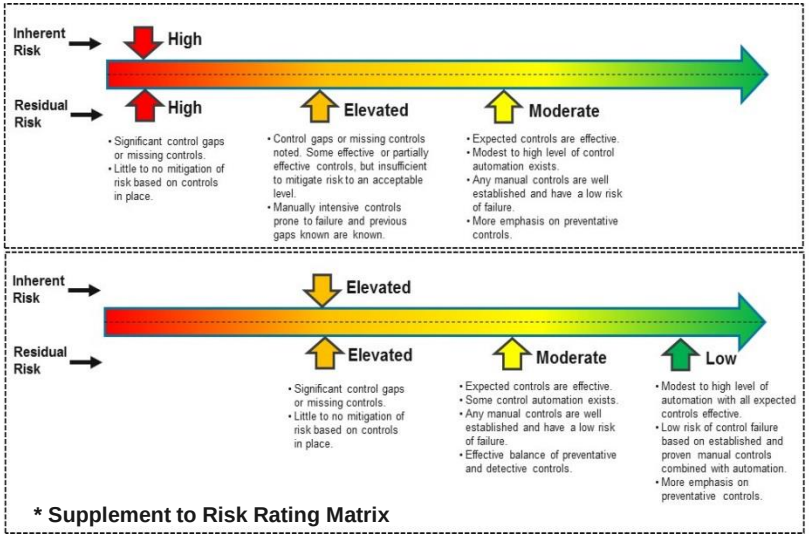
Rate Inherent Risks:

- Each risk is rated using a simplified residual risk rating approach.
- The AIG Operational Risk Rating Methodology is leveraged.

Justify Decisions:

- Rationale are required for ratings with focus on risks deemed Low/Moderate.

Residual Risk Guide



*** Supplement to Risk Rating Matrix**

Residual Risk Assessment

Risk		RCSA Residual Risk Assessment	
Risk Level 3	Risk Level 3 Description	Residual Risk Rating	Residual Risk Rating Rationale
Channel Strategy and Distribution:	Product offerings do not reach intended markets effectively and/or are misunderstood or misinterpreted.	Elevated	
Terminate Third Party Relationships:	Third party relationships are terminated improperly.	Low	
Legal contracts & agreements:	Risk associated with all contracts, e.g., contract wording, reflecting business terms, review and approval, unauthorized individuals signing contracts.	Moderate	

5. Assess Residual Risks, cont'd

Residual Risk estimates the remaining or actual risk exposure that an organization faces based on the strength of the current control environment. Residual risk is assessed after all mitigating controls are evaluated to determine how effective they are in mitigating the risk to an acceptable level (currently defined as "Moderate" risk). Higher residual risk ratings are used to prioritize control gaps requiring remediation.

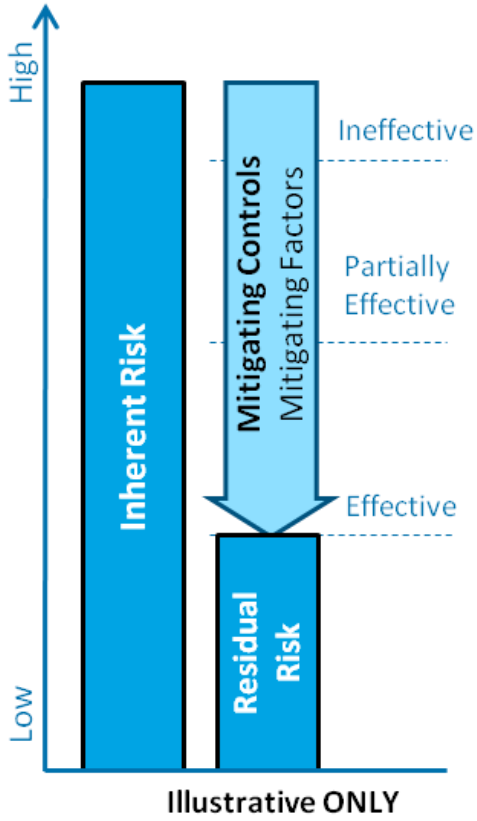
NOTE: The steps for assessing residual risk are very similar to inherent risk with one major difference, the current control environment is taken into consideration when determining impact and likelihood.

Determining Residual Risk and Subsequent Actions

- Using the ORM Risk Rating Matrix in conjunction with the supplemental guide on the next slide, assessors evaluate **Residual Risk Impact** and **Residual Risk Likelihood** for each risk and determine **Residual Risk Rating.**
- Residual risks rated as **High** or **Elevated** require creation of issues and action plans to remediate control gaps and reduce residual risk to an acceptable level (M or L).

Considerations on Residual Risk Ratings and Rationales

- For any given risk, Residual Risk should be less than, or equal to, Inherent Risk
- It should not be assumed that **residual risk impact** would be the same as **inherent risk impact**. Unlike inherent risk, residual risk takes into account controls. Therefore, impact may be less severe. For example:
  - Controls in place may reduce the volume of transactions or records (e.g. policies, claims, customers) impacted
  - Controls may detect a failure before inherent extent of impact is realized
- Ineffective and partially effective mitigating controls would not be expected to result in a substantial reduction to residual risk
- Residual risk ratings rationales should be clear and concise explaining in detail how the effectiveness of corresponding controls led to the residual risk rating determination.
- Issue and action plans are created at the control level since it is the control(s) that requires remediation to mitigate the risk.



5. Assess Residual Risks, cont'd

1 Inherent Risk

PRC Risk	Inherent Risk Rating
Risk associated with improper pricing methodologies, design or build of rating tools, tariff analysis and construct, and pricing calculations or rationale.	HIGH

2 Control Evaluation Results

PRC Expected Controls	Control Rating
Pricing for products and services (and pricing changes) are established by authorized individuals/groups and are applied to accounts and transactions in a accurate and timely manner.	Effective
Pricing and/or exposure data, rationale and pricing decisions are documented and securely stored.	Partially Effective
Automated / Manual controls are implemented to prevent inaccurate and/or unauthorized processing (e.g. warning messages to prevent double recording of claims, system checks for reasonableness of entered data, enforcement of authorities).	Effective
Delegation of authority and related limits that define approval levels for transactions are documented and periodically reviewed	Partially Effective
Management has a quality control program in respect of all significant processing activity including peer reviews, sample checking and specific audit reviews. Results and scope should be regularly reviewed and documented by management.	Partially Effective
Exceptions are properly identified, researched, escalated and resolved in a timely and appropriate manner. Processes exits to monitor the status and resolution of exceptions in accordance with policy and procedures	Partially Effective

3 Residual Risk

Residual Risk Likelihood	Residual Risk Impact	Residual Risk Rating	Residual Risk Rationale
2- Possible	3 - Elevated	ELEVATED	Residual risk determined to be Elevated. The controls in place are not effective in mitigating the risk. Key controls around u/w guidelines and authorities are in place and effective to reduce impact across categories. However, this reduction is limited as there are general inconsistencies in effectiveness of other controls needed to bring risk down to an acceptable level.

(Archer Fields)

6. Determine Risk Treatment

(RCSA Standard) Control gaps contributing to **residual risks rated as of High or Elevated are prioritized for remediation**. Ineffective and/or partially effective expected controls would not typically result a reduction of residual risk to Low or Moderate as these controls were previously identified as required for adequate mitigation. Therefore, **all control failures noted in the RCSA generally require an appropriate risk treatment** (remediation/acceptance). Management must **identify action plans** to mitigate the risk within a reasonable time period, **or in very rare cases, Management may opt not to remediate a control deficiency and accept the associated risk**. Risk acceptance follows the AIG Operational Risk Acceptance process.

Purpose:

- Document control gaps and failures noted (e.g. Issues).
- Select risk treatment (e.g. remediate vs. accept).

Develop Actions Plans (Remediation):

- Expected treatment for control gaps.
- Must include clear description of remediation plan, assign ownership, and reasonable timeline.
- Subject to IAM Standard.

File Risk Acceptance:

- Should employed in rare instances where remediation is not practical.
- Requires justification (e.g. cost benefit) and senior management approval.
- Subject to Risk Acceptance Standard.

7. Analyze, Report, and Monitor (process to be established)

A governance model inclusive of analysis, reporting, and monitoring will be developed as deployment of the new RSCA process progresses. The simplification of RCSA methodology, expansion of global scope, and implementation of an effective IT enabler will enhance reporting capabilities and drive insights into operational risks. Primary objectives are outlined below and apply to both 1st line and 2nd line.

Purpose:

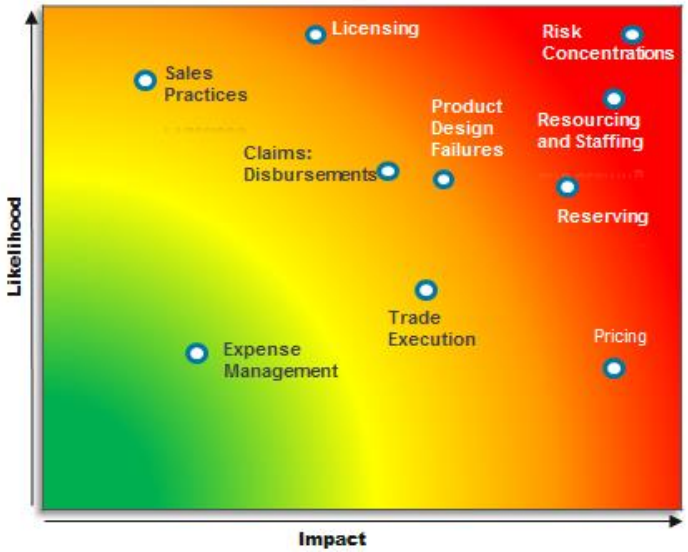
- Monitor RCSA progress and report results, at various level
- Analyze results for risk-based decision making including horizontal analysis.
- Monitor remediation plans through resolution.

Enhanced Reporting and Analytics:

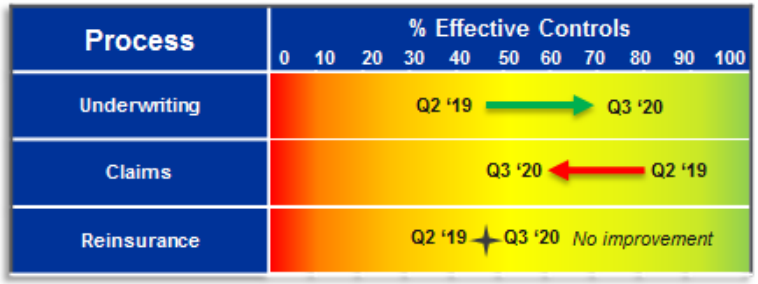
- Holistic views of risks and controls across organization, product and geography supporting aggregate risk profiles for lines of business units i.e., GI, L&R, etc.
- Availability of information critical to risk-based decision making.
- Identification of pervasive issues across geographies and product lines.
- Top Risk identification.

Analysis and Reporting Examples

Risk Heat Maps (Inherent and Residual)



Control Effectiveness Monitoring



Q&A