



# **GRC & CYBER RISK QUANTIFICATION**

## ***A STORY OF POSITIVE CO-DEPENDENCY***

**Yiannis Vassiliades, Chief Product Officer**

**Jack Whitsitt, Director of Cyber Risk Quantification**

July 12, 2023



# INTRODUCTION: CO-DEPENDENCY of CRQ and GRC?



**PREMISE:** CRQ isn't (just) a "program" or a "function", it's is way of looking at risk. Specifically, *CRQ provides a set of practices necessary for the systematic application of measurement and scientific rigor to decision making, governance, and consensus management"*

This *value proposition significantly overlaps with what happens within GRC* – to the point where a green-field organization may view them as inseparable.

*What do we mean and why does this matter? Glad you asked!*



## GRC:

A coordinated strategy for managing an organization's overall governance, risk management, and compliance with regulations. An effective GRC strategy provides a holistic, structured approach to aligning IT with business objectives, managing risk effectively, and achieving compliance with relevant laws and regulations, thus enhancing decision-making, streamlining processes, and reducing costs.

**Governance** is the process of aligning a company's strategies, policies, and procedures to meet its objectives. It involves the decisions and directions taken by the board of directors or other governing body.

**Risk Management** is the practice of identifying potential risks in advance, analyzing them, and taking precautionary steps to reduce or curb the risk.

**Compliance** ensures that organizations align with external laws, regulations, and standards, as well as internal policies and procedures.

### • GRC VALUE PROPOSITION

- **Enhanced Decision-making:** GRC provides leadership with the necessary information to make informed decisions about strategic direction and resource allocation.
- **Risk Mitigation:** Through risk management, GRC helps businesses identify, assess, and mitigate risks, reducing potential losses and improving business resilience.
- **Regulatory Compliance:** Compliance management helps prevent legal issues, penalties, and reputational damage associated with non-compliance.
- **Operational Efficiency:** By aligning processes and eliminating redundant tasks, GRC can improve operational efficiency and reduce costs.
- **Stakeholder Trust:** Adherence to GRC principles can build stakeholder trust and reputation, which can help attract customers, partners, and investors.
- **Improved Performance:** With better governance and management of IT resources, GRC can contribute to improved performance and achievement of business objectives.



# GRC Practice Area 1: Risk Identification and Definition



Objective Setting: Define the business objectives and compliance requirements.

Inputs: Business strategy, regulatory requirements

Outputs: Defined business and compliance objectives

Risk Inventory Development: Develop a risk register or inventory to track identified risks.

Inputs: Identified risks from various sources

Outputs: Risk register

Risk Treatment Strategy: Develop strategies to treat identified risks, such as mitigation, acceptance, or transfer. Identify applicable control frameworks.

Inputs: Risk register, risk appetite, business objectives

Outputs: Risk treatment strategy, selected control frameworks



# GRC Practice Area 2: Risk Governance

Risk Appetite and Tolerance Definition: Define the organization's risk appetite and tolerance levels.

Inputs: Business strategy, risk insights, stakeholder expectations

Outputs: Defined risk appetite and tolerance levels

Decision-Making Criteria and Consequence Modeling: Set criteria for risk-related decisions and develop models to predict the consequences of different decisions.

Inputs: Risk appetite, risk treatment strategy, business objectives

Outputs: Decision-making criteria, consequence models

Risk Management Strategy Development: Formulate a strategy for managing risks based on the defined risk appetite, decision-making criteria, and consequence models.

Inputs: Decision-making criteria, consequence models, risk insights

Outputs: Risk management strategy





# GRC Practice Area 3: Risk Management Execution

Risk Assessment: Carry out risk assessments to understand the nature and magnitude of identified risks.

Inputs: Risk register, risk management strategy

Outputs: Risk assessment reports

Risk Scoring: Score or rank risks based on their potential impact and likelihood.

Inputs: Risk assessment reports

Outputs: Risk scores

Risk Reporting: Document and report on the identified risks, their scores, and potential impact.

Inputs: Risk scores, risk assessment reports

Outputs: Risk reports

Analysis and Planning: Analyze risk reports and plan appropriate responses.

Inputs: Risk reports

Outputs: Risk response plan

Risk Response: Implement the planned responses to the identified risks.

Inputs: Risk response plan


Outputs: Implementation reports, updated risk register

Risk Monitoring: Continuously monitor and review the identified risks, the effectiveness of the responses, and the risk environment.

Inputs: Implementation reports, updated risk register

Outputs: Risk monitoring reports, updates to risk register and risk management strategy





**CYBER RISK QUANTIFICATION:** Provides an objective view of an organization's cyber risk landscape. Instead of relying on subjective, qualitative ratings, CRQ uses statistical techniques and data analysis to evaluate potential loss magnitude and frequency. This method fosters more informed decision-making by providing specific data points and metrics rather than broad, subjective categories.

## INPUT VALUE PROPOSITIONS

**CRQ Scenarios:** A broadly comprehensive sample set of baseline scenarios can provide an organizing principle that ties together risk related information & assumptions into a common framework of control opportunities & objectives, policy testing frameworks, business dependencies, risk stressors, etc. helps assure risk management activities remain coordinated in a common strategy

**CRQ Estimation Models:** The act of identifying data sources of record and eliciting knowledge for CRQ quantification can provide clear insights into existing "visibility risk" an organization faces. It can also help clarify what metrics are needed, the meaning of existing metrics – as well as contribute to the development, refinement, and targeting of assessment tools and processes.

## OUTPUT VALUE PROPOSITIONS

**Target outcomes for information security decisions:** When considering new investments, adopting new services, or responding to cyber threats, CRQ can provide quantified estimates of potential losses, enabling more informed decision-making based on how these estimates compare to the organization's risk appetite, tolerance, and thresholds.

**Quantified risk metrics:** not only provide a common language for communication but also enhance overall governance. They allow risk reports to show where estimated losses from CRQ scenarios fall relative to the defined risk appetites, tolerances, and thresholds, making it easier for decision-makers to understand where attention and resources are required.

**The science-based, rigorous measurement practices embodied by CRQ can – and should – inform overall decision making and risk management processes.**



# CRQ Decomposed: What information is pertinent to what aspect of CRQ?



	SCENARIO SELECTION	SCENARIO CONSTRUCTION	DATA SOURCING	REPORTING	ANALYSIS & DECISION SUPPORT
Appetites & Governance Models					
Business & Control Stressors					
Business & Technical Projects and Changes					
Business Objectives					
Control Implementation & Performance Characteristics					
Control Strategies					
Cyber Threat Events					
Gaps and Concerns					
Key Metrics, KPIs, KRIs					
Key Technology, Data, and Human relationships					
Policies & Standards					
Policies					
Threats to Objectives					
Consensus Models of the Environment					

All of this information is exceedingly co-dependent and it would not be incorrect to suggest that it all can influence every aspect of your CRQ work.





# BI-DIRECTIONAL RELATIONSHIP: CRQ Provides scientific and measurement rigor, GRC provides information and context

## GRC PROCESSES AND OUTPUTS

### RISK IDENTIFICATION AND DEFINITION

- **Objective Setting:** Defined business and compliance objectives
- **Risk Inventory Development:** Risk register
- **Risk Treatment Strategy:** Risk treatment strategy, selected control frameworks

### RISK GOVERNANCE

- **Risk Appetite and Tolerance Definition:** Defined risk appetite and tolerance levels
- **Decisioning Models:** Decision-making criteria, consequence models
- **Risk Management Strategy Development:** Risk management strategy

### RISK MANAGEMENT EXECUTION

- **Risk Assessment:** Risk assessment reports
- **Risk Scoring:** Risk scores
- **Risk Reporting:** Risk reports
- **Analysis and Planning:** Risk response plan
- **Risk Response:** Implementation reports, updated risk register
- **Risk Monitoring:** Risk monitoring reports, updates to risk register and risk management strategy



## INFORMATION PERTINENT TO CRQ

Appetites & Governance Models

Business & Control Stressors

Business & Technical Projects and Changes

Business Objectives

Control Implementation & Performance Characteristics

Control Strategies

Cyber Threat Events

Gaps and Concerns

Key Metrics, KPIs, KRIs

Key Technology, Data, and Human relationships

Policies & Standards

Policies

Threats to Objectives

Consensus Models of the Environment



# (SOME) INTEGRATED VALUE PROPOSITIONS

## RISK IDENTIFICATION AND DEFINITION

- Objective Setting:** CRQ provides value here by quantifying Business Objectives, using Key Metrics, KPIs, and KRIs. This helps in setting targets that align with risk appetites and governance models.
- Risk Inventory Development:** Cyber Threat Events, Threats to Objectives, and Gaps and Concerns are made explicit and quantified. This allows a comprehensive view of the risk landscape and aids in the development of a more robust risk register.
- Risk Treatment Strategy:** Control Strategies are critically evaluated based on their ability to address identified risks. Control Implementation & Performance Characteristics are also considered, ensuring the strategies chosen are feasible and effective.

## RISK GOVERNANCE

- Risk Appetite and Tolerance Definition:** Appetites & Governance Models are quantified and made explicit, providing a clear, consensus-based understanding of the organization's risk tolerance.
- Decisioning Models:** CRQ brings consensus to Decisioning Models by incorporating explicit Policies & Standards and considering the potential impact of Business & Technical Projects and Changes. This helps in developing a model that is broadly agreed upon and fits the organization's risk profile.
- Risk Management Strategy Development:** CRQ provides value here by ensuring the strategy is in line with quantified Business Objectives, Appetites & Governance Models, and addresses identified Threats to Objectives.

## RISK MANAGEMENT EXECUTION

- Risk Assessment:** Using CRQ, organizations can make the implicit assumptions in their risk assessments explicit, thus improving their scientific rigor. The assessments become data-driven, considering Business & Control Stressors, Cyber Threat Events, and Gaps and Concerns.
- Risk Scoring:** The use of Key Metrics, KPIs, and KRIs in CRQ brings consistency and objectivity to the risk scoring process, ensuring risks are ranked based on their true potential impact.
- Risk Reporting:** CRQ allows for the clear communication of risk in reports, backed by quantified data. It ensures the organization's consensus model of the environment is reflected in these reports.
- Analysis and Planning:** CRQ provides a way to quantify and make explicit the potential effects of different risk responses. This is critical in the development of a robust and effective risk response plan.
- Risk Response:** The CRQ process ensures responses are grounded in clear, quantifiable understanding of Control Implementation & Performance Characteristics and Control Strategies.
- Risk Monitoring:** By providing quantified updates to the risk register and the risk management strategy, CRQ allows for effective risk monitoring. The use of Consensus Models of the Environment ensures that changes in the risk landscape are promptly reflected in the organization's risk management approach.

**TLDR: Review your GRC program against CRQ practices. Use GRC in CRQ. Maintain Alignment.**



# "Risks" of Dissonance

## Inadequate Scientific/Measurement

- An internal audit team may overlook key risks because the qualitative risk assessment process failed to identify them. This could leave the organization vulnerable to significant risk events.
- The board of directors may make strategic decisions based on incomplete or inaccurate risk information due to lack of rigorous risk assessment, potentially compromising the organization's long-term health.
- A risk manager might overestimate the potential impact of a low risk due to imprecise risk measurement, leading to unnecessary expenditure on mitigation efforts.
- The organization might underestimate a significant risk due to vague risk measurements, resulting in insufficient resources being allocated to its management.
- A compliance officer might fail to accurately assess regulatory risks due to imprecise risk measurements, potentially leading to non-compliance penalties.

## Poor Consensus Management

- The risk management department may develop a risk management strategy that isn't fully aligned with the business objectives IN A RISK CONTEXT because of differing perceptions of these objectives.
- Different departments might set conflicting KPIs due to diverging understandings of business objectives IN A RISK CONTEXT, leading to inefficiencies and confusion.
- Senior executives may approve a project with a risk level that exceeds the organization's risk appetite because of a misaligned understanding of the risk appetite.
- A department might pursue an opportunity that is outside the organization's risk appetite due to a misalignment in understanding, potentially exposing the organization to unnecessary risks.
- The board might not be able to effectively oversee risk management if their understanding of risk appetite doesn't align with that of the risk management team, potentially leading to strategic errors.





**JOIN US FOR OUR NEXT WEBINAR:  
PRACTICAL APPLICATIONS OF THE  
GRC & CRQ RELATIONSHIPS**

**AUGUST 2, 2023**

**[WWW.OSTRICHCYBER-RISK.COM/EVENTS](http://WWW.OSTRICHCYBER-RISK.COM/EVENTS)**

