Ostrich Cyber-Risk

4 STEPS TO SEC “COMPLIANCE”

Jack Whitsitt | Director of CRQ

Jack.Whitsitt@ostrichcyber-risk.com

Hello!

Ostrich Cyber-Risk

- “4 Steps To SEC Compliance”: Maybe a bit of a misnomer?
- More accurate: “4 Stages of Risk Governance…that probably really help with new SEC rule compliance!”
- The former is easier to say and process. ☺
- Easy TLDR: Do CRQ and then use the results! (True, but ??)
- Super high level is not the same as generic: Mistakes often made by not looking at the whole system
- Better TLDR: Pay attention to how the steps support each other bi-directionally.
- Steps: 3 things the SEC asks for and 1 they should have.
- Let’s start with the end and work backward!

Brief Review of the new SEC rules

Ostrich Cyber-Risk

- i) Form 8-K disclosure of material cybersecurity incidents within four (4) business days of the company's determination that the cybersecurity incident is material;
- (ii) new annual disclosures in Form 10-K regarding the company's cybersecurity risk management and strategy, including with respect to the company's processes for managing cybersecurity threats and whether risks from cybersecurity threats have materially affected the company;
- (iii) new annual disclosures in Form 10-K regarding the company's cybersecurity governance, including with respect to oversight by the board and management.

Step 4: Reporting Material Failures

Ostrich Cyber-Risk

…disclosure of material cybersecurity incidents within four (4) business days of the company's determination that the cybersecurity incident is material; …material aspects of the nature, scope, and timing of the incident, and the material impact or "reasonably likely" material impact on the company, including on its financial condition and results of operations…

Step 4: Reporting Material Failures

Ostrich Cyber-Risk

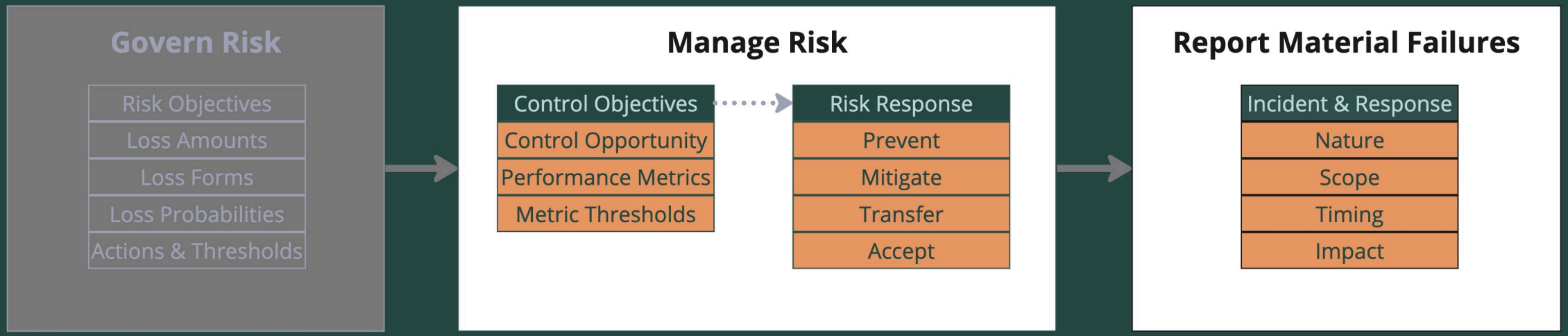
What is reported should convey information necessary for decisions to be made by key stakeholders in the business. Making decisions requires visibility confidence: Past, Current, Future states, Causes, etc

- **Nature**: Triggers | Drivers | Controls | Weaknesses
- **Scope:** Attack Chain Steps & State Changes (People | Process | Technology)
- **Timing:** Initial Attempt | First Foothold | Dwell Time | Loss Events (State Changes) | Current Status
- **Impact:** Business Event | Stakeholders | Equities| Reaction Chain | Loss Accounting | Known Loss | Forecast Loss
- *Risk Management Context: How was this event being managed and what was the RM escape?*

Step 3: Risk Management Approach

Ostrich Cyber-Risk

CONSISTENT RISK FRAME: EVENT TRIGGERS | EVENT OUTCOMES | EVENT DRIVERS | EVENT DATA



…regarding the company's cybersecurity risk management and strategy, including with respect to the company's processes for managing cybersecurity threats and whether risks from cybersecurity threats have materially affected the company; …processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes…

Step 3: Risk Management Approach

Managing risk can – and should - prepare you for reporting; what you may have to report should also be what you are managing.

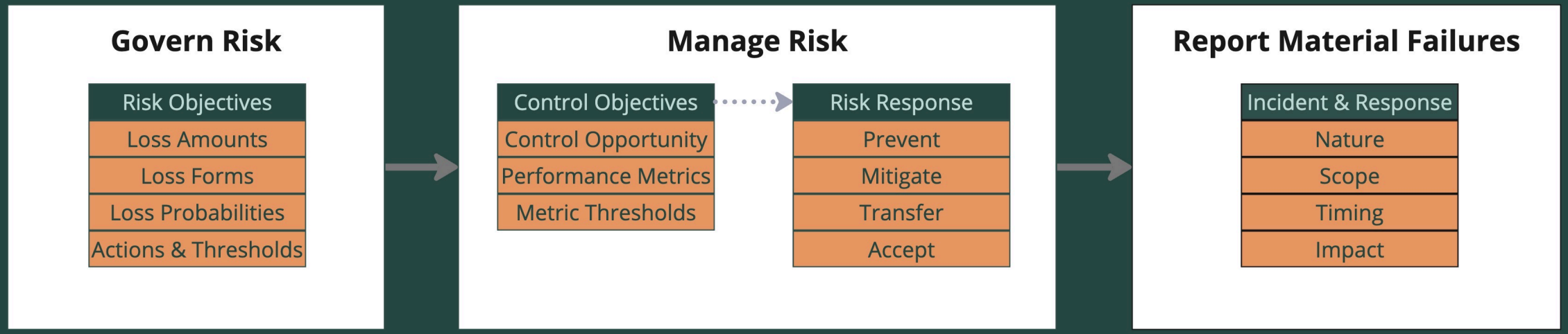
Every control objective should have a risk response.

- Each Risk Response is a control class
- Controls within control classes work cooperatively to achieve control objectives
- Control objectives are a combination of:
  - Control opportunities: Think “FAIR Factor” and “Range Elements”
  - Performance Metrics/Indicators: What about control behavior drives factor?
  - Metric Thresholds: How much performance is “enough” to mitigate “risk”?
- This requires pre-modeling

Step 2: Risk Governance Approach

Ostrich Cyber-Risk

CONSISTENT RISK FRAME: EVENT TRIGGERS | EVENT OUTCOMES | EVENT DRIVERS | EVENT DATA



…the company's cybersecurity governance, including with respect to oversight by the board and management…..describe the board of directors' oversight of risks from cybersecurity threats. If applicable, companies must identify any board committee or subcommittee responsible for the oversight of risks from cybersecurity threats and describe the processes by which the board or such committee is informed about such risks.

Step 2: Risk Governance Approach

- **Loss Amount:** How much loss is too much?
- **Loss Forms:** How is loss ”Counted”?
- **Loss Probabilities:** How probable is “too” probable?
- **Action Thresholds:** What actions will be taken when by whom?

Governing risk entails tying risk to business objectives and success metrics and assuring objectives are met.

“Risk Limits” define the maximum amount of loss acceptable and the acceptable probability of that loss given business objectives and success metrics

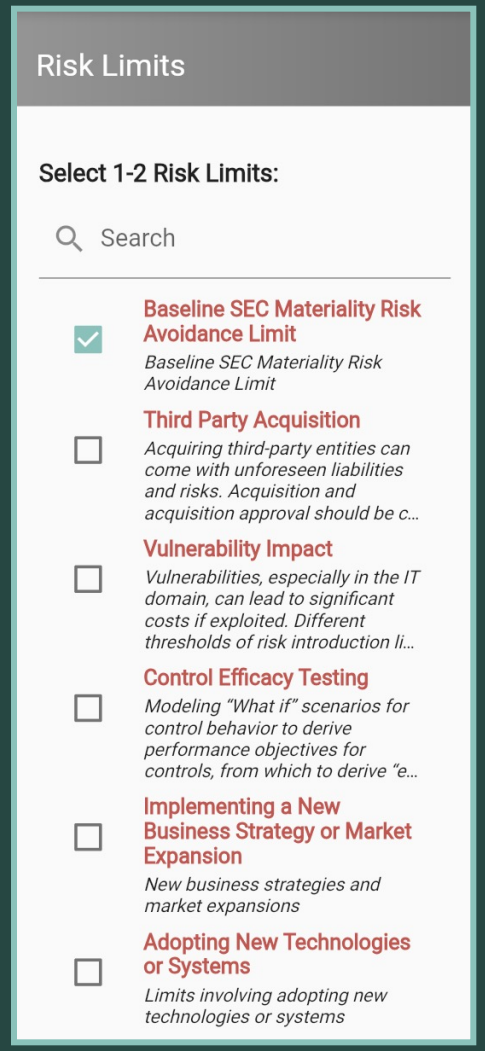
“Risk Limits” can refer to Risk Appetites, Tolerances, and Thresholds as they pertain to specific decision contexts

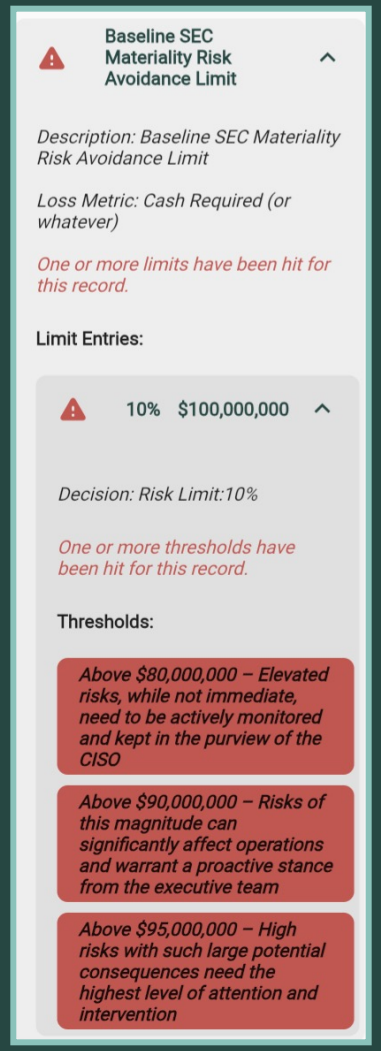
“Materiality” can be a stated “Tolerance” and governance routines can be defined as Actions to be taken when risk reaches a “Threshold” as it approaches a “Tolerance”

“Loss” can be a generic term – what does it actually mean in terms of constrained resources, business goals, and stakeholder equities?

Step 2 Detail: Quantified Risk Limits | "Storm Model"

Ostrich Cyber-Risk

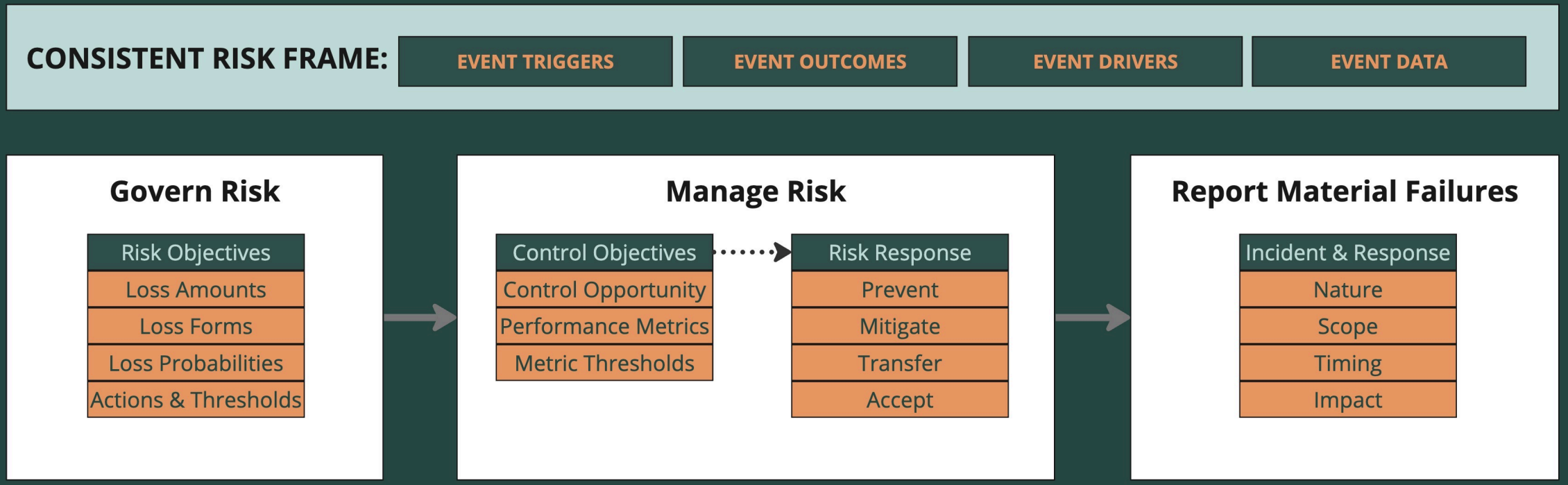




Percentile	Risk Forecast	Baseline SEC Materiality Risk Avoidance Limit
0.01%	$1,026,593,123	
0.1%	$837,639,769	
1%	$588,429,991	
5%	$383,114,254	
10%	$298,878,729	$100,000,000
25%	$178,168,989	
50%	$88,448,142	
75%	$37,102,132	
90%	$14,213,393	
95%	$7,176,145	
99%	$1,404,188	
99.9%	$88,387	
99.99%	$15,040	

Step 1: Architect a Consistent Risk Frame

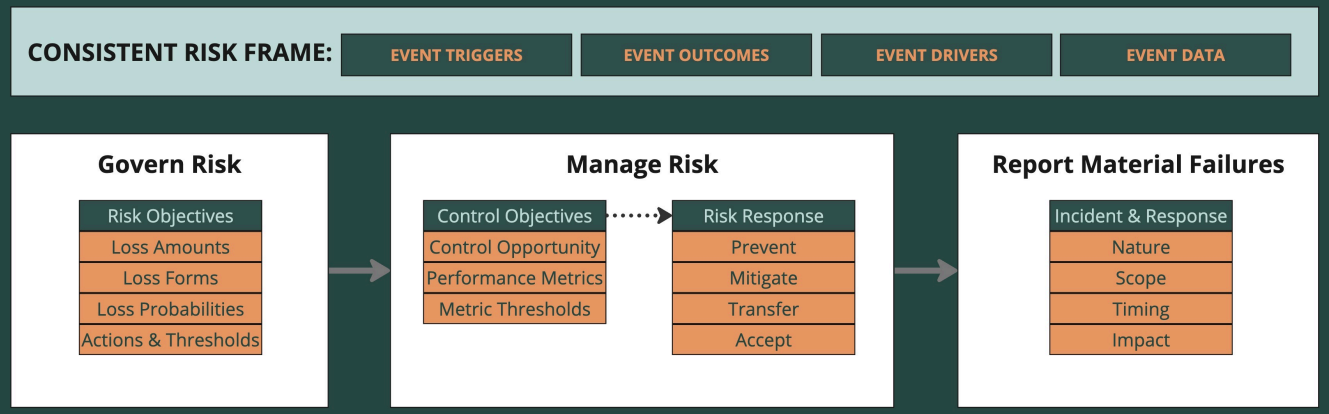
Ostrich Cyber-Risk



...material aspects of the nature, scope, and timing of the incident, and the material impact or "reasonably likely" material impact on the company, including on its financial condition and results of operations...

Step 1: Architect a Consistent Risk Frame

Ostrich Cyber-Risk



At the heart of material risk governance, management, and reporting is a consistent risk frame.

A risk frame consists of the suite of contextual material loss drivers and the amount of risk they posed.

A common risk driver lexicon, documented forecasting models, a register of baseline risk scenarios, FAIR quantification practices, and "baseline forecast" CRQ approach work cooperatively to provide a risk frame.

- **Risk Frame:**
  - "Sample Scenario Index"
  - Represents breadth of risks (Dow Jones Index / Risk Register)
  - Baseline Quantified Forecasts vs "tactical" analysis
- **Event Triggers:** Classes of Threat Events used in Risk Frame
- **Event Outcomes:** Classes of Losses used in Risk Frame
- **Event Drivers:** How do the environment and controls drive risk factors?
- **Event Data:** What do we know about Event Driver behavior and the future?

Step 1 Detail: Risk Frame “Scenario” Details

Ostrich Cyber-Risk

“Risk Event-Scenario Lexicon”

EVENT TRIGGERS	EVENT OUTCOMES	EVENT (BEHAVIOR) DRIVERS			FORECASTING DATA
		FREQUENCY	SUSCEPTIBILITY	LOSS	
Key Initial Access Vectors	Key Business Events	Threat Motivation	Surface Base Rate	Pool of Value Available	Source of Record
Key Transited Assets	Event Stakeholders	Threat Objective	Control Opportunities	Event to Equity Match	Reference Class Precision
Key State Changes	Stakeholder Equities	Threat Communities	Surface Control Actions	Match Degree	Source Reliability
Key TTPs	Stakeholder Responses	Base Rate Incentives	Exploitation Control Actions	Equity Impact Degree	Data Time Relevance
Key Enabling Surfaces	Cash Spends	Control Opportunities	Control Suite Performance	Control Opportunities	Meaning for Future
	Devaluations	Contact Control Actions		Equity Match Ctl Actions	
	Cost Increases	PoA Control Actions		Match Degree Ctl Actions	
	Lost Opportunities	Control Suite Performance		Control Suite Performance	

“Baseline Risk Event-Scenario Register”

Fraud and Ransomware	Disgruntled Insider (Data Leak)
Market Manipulation	Disgruntled Insider (Disruption)
Disinformation Campaigns	Nation State Espionage (Geopolitical)
Infrastructure Sabatoge	Nation State Espionage (Industrial/Business)
Data Breaches	Hacktivism and Politics
Technical Resource Theft	Opportunistic

FAIR Scenarios (Groups of Event-Scenarios)

Ostrich Cyber-Risk

THANK YOU!
QUESTIONS?

Jack Whitsitt | Director of CRQ

Jack.Whitsitt@ostrichcyber-risk.com