metricstream

GRC SUMMIT 2022

LONDON, NOV 8-9

Hosted by MetricStream

Incorporating Risk Quantification, AI and Automation into Your CyberGRC Strategy

Gavin Anthony Grounds CEng CITP CDPSE CRISC FBCS

Sr. Director – Security, Risk & Compliance, Meta

gavingrounds
gavin.grounds
gavingrounds

Agenda

1. Qualitative versus Quantitative risk management
   – Why Quantitative Risk Management is a pre-requisite

2. Why managing solely based on Annualized Loss Expectancy and/or Risk Reduction is not enough

3. How to build and scale a quantitative cyber risk management capability for small and large organizations

4. How to maximize the value of what is already known (or easily-knowable) in a Cyber Risk Quantification model

Agenda

1. Qualitative versus Quantitative risk management
   – Why Quantitative Risk Management is a pre-requisite

2. Why managing solely based on Annualized Loss Expectancy and/or Risk Reduction is not enough

3. How to build and scale a quantitative cyber risk management capability for small and large organizations

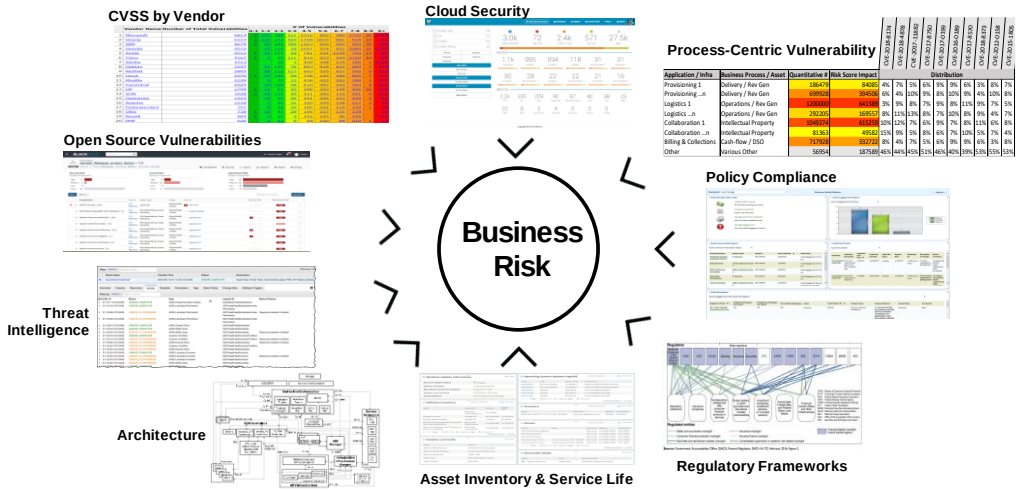
4. How to maximize the value of what is already known (or easily-knowable) in a Cyber Risk Quantification model

Qualitative versus Quantitative risk management

Qualitative Measures: Colors, Gradients and Silos

Disparate and subjective relativity scoring mechanisms, qualitative / non-quantified measures & metrics, lack of architectural, business and process contexts, lack of regulatory landscape alignment and lack of consistent threat landscape telemetry

- Risk Assessment Results:
  - Negligible / Minor / Significant / Serious / Severe
- Vulnerability Management
  - Low / Medium / High / Critical
  - Scored 1 through 10
- End of Support Life / Service Life
  - Number of Days / Weeks / Months
- Architectural & Environmental
  - Internet Connections / 3rd-party
- Regulatory scrutiny



Qualitative Method:

$$R = ra + v + e + a + s$$

If: *ra* = severe; v = critical;

e = 6 months; a = internet-facing + 3rd-Part APIs

S = PCI DSS + CCPA

Agenda

1. Qualitative versus Quantitative risk management
   – Why Quantitative Risk Management is a pre-requisite

2. Why managing solely based on Annualized Loss Expectancy and/or Risk Reduction is not enough

3. How to build and scale a quantitative cyber risk management capability for small and large organizations

4. How to maximize the value of what is already known (or easily-knowable) in a Cyber Risk Quantification model

Cyber Risk Quantification – Driving business value… “the Up-side of Risk”

Clearer, fact-based visibility delivers more effective Risk Management

Cyber Risk Quantification is a foundational **pre-requisite**.

Quantitative Method:

$$a + b < c$$

If: c = business value = $12M;

$a + b$ = risk; a = $10M

What is the Maximum allowable value of b?

Qualitative Method:

$$a + b < c$$

If: c = business value = $12M;

$a + b$ = risk; a = Medium

What is the Maximum allowable value of b? Low? / Medium? / High? / Critical?

Annualized Loss Expectancy and Risk Reduction is not enough

Objective Cannot be solely *Reducing* Risk

- Most Cyber Security Risk Quantification models focus primarily on ALE (Annualized Loss Expectancy)
  - Annual Rate of Occurrence (ARO) x Single Loss Expectancy (SLE)
  - ARO based on Likelihood (Monte Carlo Simulation) and history is almost irrelevant
  - Cyber Risk has ***intelligent*** threat actors and regulators – not just random ranges

- Risk Reduction objectives are often incompatible with Business enablement.

"You cannot effectively Enable the Business, if you only seek to reduce Risk"

❑ Will you accept $1M of risk to enable $100M of business value?

❑ Will you accept 7 Critical risks to enable $100M of business value?

Same Risk Scenario

Agenda

1. Qualitative versus Quantitative risk management
   – Why Quantitative Risk Management is a pre-requisite

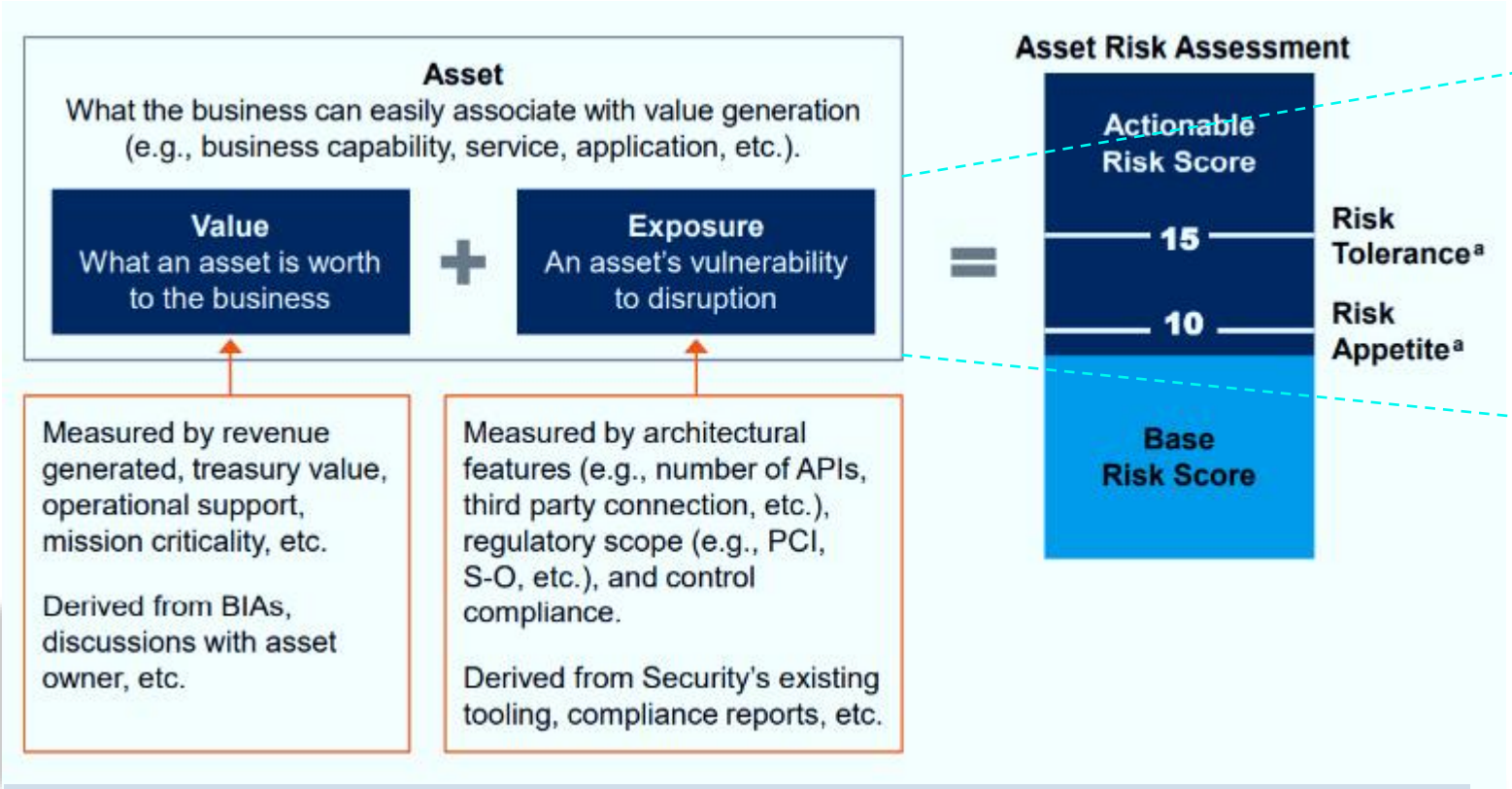
2. Why managing solely based on Annualized Loss Expectancy and/or Risk Reduction is not enough

3. How to build and scale a quantitative cyber risk management capability for small and large organizations

4. How to maximize the value of what is already known (or easily-knowable) in a Cyber Risk Quantification model

Ground Cyber Risk Quantification in Assets, Not Scenarios

"Grounds' Rules" – Asset-based Cyber Risk Quantification Approach



All the information needed to quantify asset risk is trustworthy, known or easily knowable.

The enterprise's asset inventory is finite, making cyber risk quantification manageable at the enterprise scale.

Use of existing control monitoring capabilities lets asset owners see exposure in real-time.

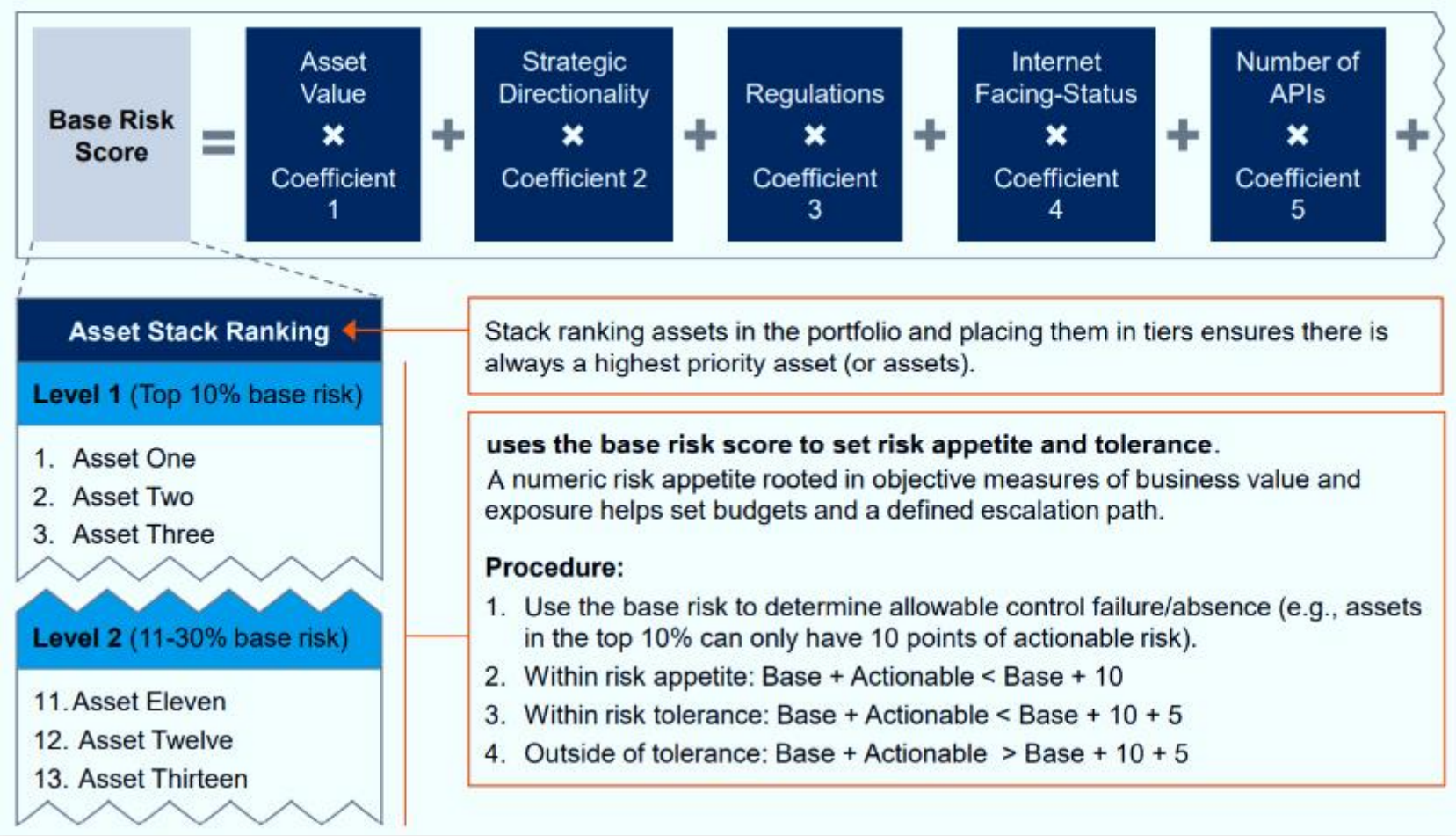
Grounds' Rules for Cyber Risk Quantification:

"Start with what you do know, improve on what you could know, aspire to what you should know."

** Source: Adapted from Gartner. Case Study on Verizon and "Grounds' Rules" method.*

Comprehensive Cyber Risk Quantification – How to scale & deliver Business Value

"Base-Risk" Quantification

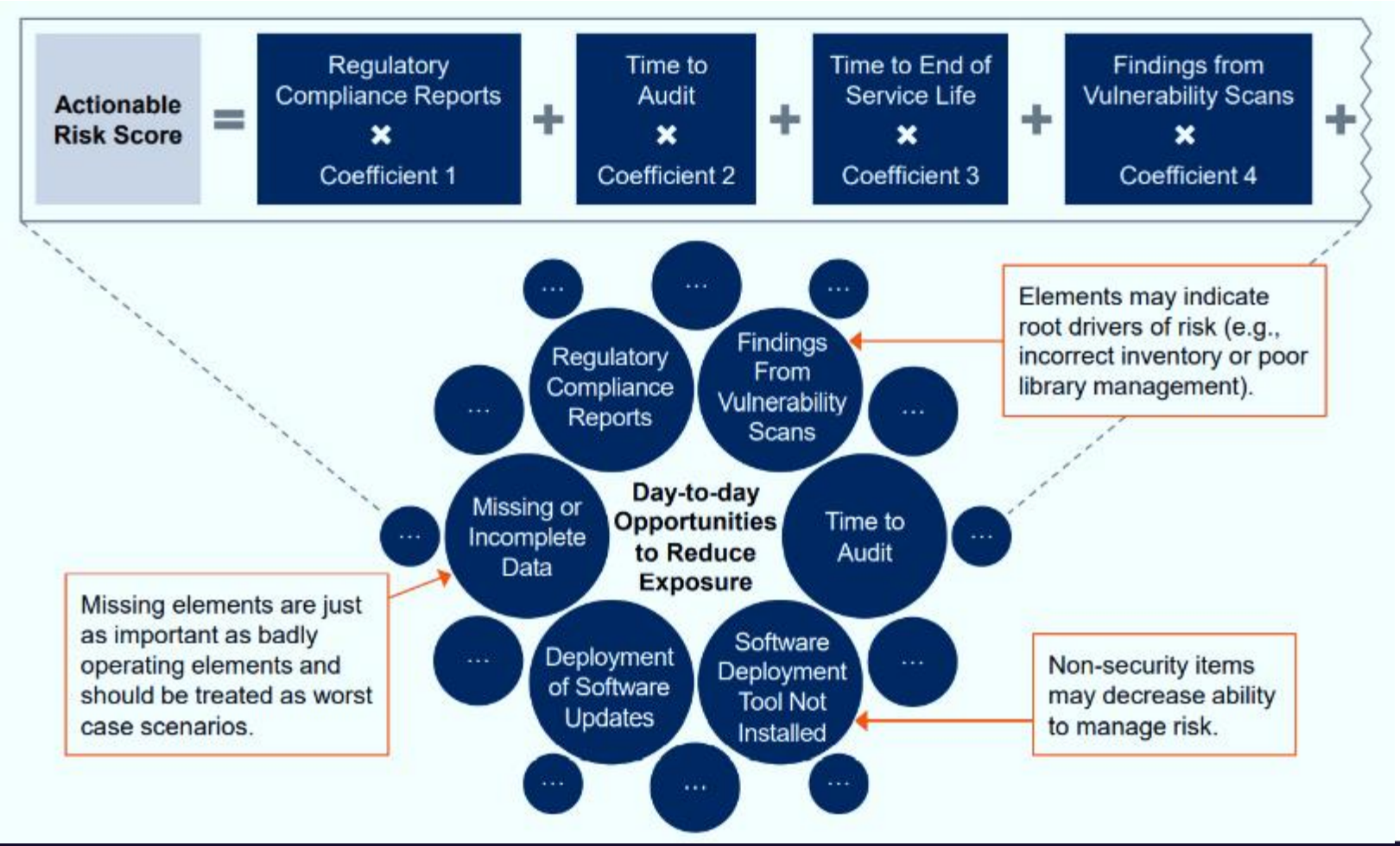


** Source: Adapted from Gartner. Case Study on Verizon and "Grounds' Rules" method.*

**** illustrative data only***

Comprehensive Cyber Risk Quantification – How to scale & deliver Business Value

"Actionable-Risk" Quantification



** Source: Adapted from Gartner. Case Study on Verizon and "Grounds' Rules" method.*

**** illustrative data only***

Comprehensive Cyber Risk Quantification – How to scale & deliver Business Value

Link Action Options Explicitly to Exposure Reduction

Actions to Drive Down Actionable Risk	Score[a]
Address critical findings from vulnerability scans	-3
Accelerate asset refresh due to time to end of service life	-2
Conduct a soft audit	-2
Shift from manual to automated software updates	-1
Install vulnerability scanning	-1
Install logging capability	-1

Actions to Drive Down Base Risk
Update asset operating system
Reduce data retention in the asset
Disconnect asset from public networks

** Source: Adapted from Gartner. Case Study on Verizon and "Grounds' Rules" method.*

**** illustrative data only***

Agenda

1. Qualitative versus Quantitative risk management
   – Why Quantitative Risk Management is a pre-requisite

2. Why managing solely based on Annualized Loss Expectancy and/or Risk Reduction is not enough

3. How to build and scale a quantitative cyber risk management capability for small and large organizations

4. How to maximize the value of what is already known (or easily-knowable) in a Cyber Risk Quantification model

Comprehensive Cyber Risk Quantification – How to scale & deliver Business Value

'Go to War With the *[Data]* You Have'

Maximize and Leverage the detailed information already available

- Asset Inventory
  - Incomplete / Inaccurate is better than nothing
- Architectural Information
- Business Function Value and Mission Criticality
- Data Classifications and Relative Data Value
- Compliance Information and Monitoring & Audit Findings
- KPIs and Performance Metrics from Active Controls
- Missing data, in of itself, is a measurable metric
- Root Cause Analyses
  - Operations and Security Related
- Legal, Contractual & Regulatory Obligations

Manage Information / Cyber Security Risk as a Risk Currency

Establish consistent relative numeric and quotients, grounded in business contexts

"The only place you can start from, is where you are and from the path that you're on."
– Gavin Anthony Grounds

Cyber Risk Quantification – Key Takeaways

Objective Cannot be solely ***Reducing*** Risk

- Quantification of Cyber Security Risk is a pre-requisite for effective, business-oriented risk management

- Annualized Loss Expectancy and Risk Reduction strategies are not enough
  - Monte Carlo Simulations and historical trends alone are not effective for modeling likelihood in Cyber Risk

- You can only start from where you are and from the path that you are on –
  - Quantifying Something is better than quantifying Nothing
  - “Perfection is the Enemy of Progress” (Sir Winston Churchill)

- ***“Start with what you DO know, improve based on what you COULD know, and aspire to what you SHOULD know”*** (Gavin Anthony Grounds)

Q & A

gavingrounds
gavin.grounds
gavingrounds

Recommended Reading and Sources

Case Study: Verizon's Cyber Risk Quantification Program
Gartner Cybersecurity Research Team (G00760138)

Systems and Methods for Automated Quantitative Risk and Threat Calculation and Remediation
Gavin Anthony Grounds; David R. Grantges (US Patent # 20210266340)