GRC SUMMIT 2023

MIAMI, JUNE 14 & 15

Hosted by MetricStream

EXPERIENCE
the Power of Connection

GRC
SUMMIT 2023
MIAMI, JUNE 14 & 15
Hosted by MetricStream

Incorporating Risk Quantification, AI, and Automation into Your Cyber Risk Strategy

Gavin Anthony Grounds MBA CEng CITP FBCS CRISC CDPSE CISSP

CEO & Co-founder. Mercury Risk and Compliance, Inc.

Agenda

- Qualitative versus Quantitative risk management
  – Why **Quantitative** Risk Management is a **pre-requisite** for the business

- Why managing solely based on **Annualized Loss Expectancy** and/or **Risk Reduction** is **<u>not</u>** Real Risk Management
- ***How*** to **build and scale** a quantitative cyber risk management capability for small and large organizations using automation and AI
- **How** to maximize the value of what is ***already known*** (or easily-knowable) in a Cyber Risk Quantification model
- Audience Questions and Discussion

Agenda

- Qualitative versus Quantitative risk management
  – Why **Quantitative** Risk Management is a **pre-requisite** for the business

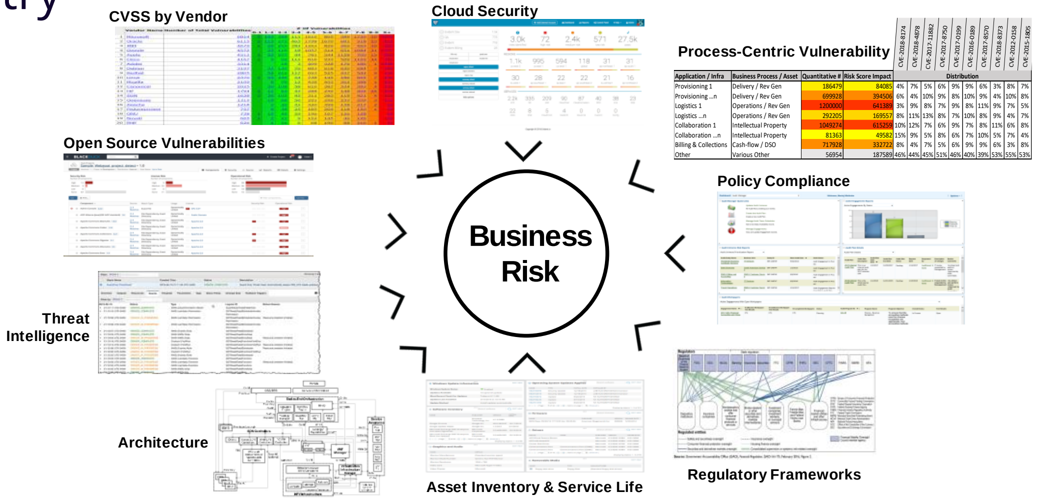
- Why managing solely based on **Annualized Loss Expectancy** and/or **Risk Reduction** is **not** Real Risk Management
- ***How*** to **build and scale** a quantitative cyber risk management capability for small and large organizations using automation and AI
- **How** to maximize the value of what is ***already known*** (or easily-knowable) in a Cyber Risk Quantification model
- Audience Questions and Discussion

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

- Qualitative versus Quantitative risk management
  – Why **Quantitative** Risk Management is a **pre-requisite** for the business

- Why managing solely based on **Annualized Loss Expectancy** and/or **Risk Reduction** is **not** Real Risk Management
- ***How*** to **build and scale** a quantitative cyber risk management capability for small and large organizations using automation and AI
- **How** to maximize the value of what is ***already known*** (or easily-knowable) in a Cyber Risk Quantification model
- Audience Questions and Discussion

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?

Exclusively focusing on Reducing Risk and ALE is NOT Risk Management

Clearer, fact-based visibility delivers more effective Risk Management

- Annualized Loss Expectancy (ALE) =
  - Annual Rate of Occurrence (ARO) x Single Loss Expectancy (SLE)
  - ARO based on Likelihood, regression models (Monte Carlo Simulation) and historical performance – in Cyber and Technology Risk is all but irrelevant
  - Cyber and Technology Risk has intelligent threat actors and regulators – not just random events and ranges

- NOTABLY:: It is **impossible to reduce risk**.
  - We can reduce likelihood
  - Risk = Consequence (or potential consequence).
    - We can ***exchange*** consequences, but we can't eliminate consequences.
  - An effective Board of Directors is not expecting risk avoidance – it expects to be informed as to what risk we ***should*** take to meet business objectives and deliver returns on risk

Trigger Warning

- The next section discusses motorcylce accidents and related physical, mental and/or emotional trauma

“Real” Risk Management – Case Study

“Petrol-Head” Grounds Brothers

Gavin

Darren

“Real” Risk Management – Case Study

Darren

“Real” Risk Management – Case Study Darren

- There is NO such thing as “Risk Reduction” – only a risk exchange
    - Darren could reduce the risk of death by implementing controls such as slowing down, wearing safety equipment, etc.
- Slowing down <u>decreases</u> ***likelihood*** of an accident which could result in death
- Slowing down <u>increases</u> ***likelihood*** that the race will be lost
    - It is a risk EXCHANGE, not a risk reduction
- Wearing safety equipment EXCHANGES the risk (consequence) from death to a different suite of risks, such as intensive care and medical bills.
- Focusing exclusively on risk of loss increases likelihood of failing to win
- In business, the objective of risk management is to optimize risk in order to win

Exclusively focusing on Reducing Risk and ALE is NOT Risk Management

Clearer, fact-based visibility delivers more effective Risk Management

- Risk = (Potential) Consequence
- There is no such thing as data loss risk
  - Data loss is an **outcome** or an **issue**
  - The **risk = the consequence(s)** because of the data loss.
  - Implementing effective controls does not reduce risk
    - It can reduce likelihood
    - It can exchange the consequence (risk) for another consequence or suite of consequences (risks)
  - There is no such thing as a "high risk vulnerability"
    - We might have highly exploitable vulnerabilities, but the risk level is based on the consequence(s) (Risk(s)) that would be realized if the vulnerability were to be exploited

- NOTABLY:: It is **impossible to reduce risk**.
  - We can reduce likelihood
  - Risk = Consequence (or potential consequence).
    - We can ***exchange*** consequences, but we can't eliminate consequences.
  - An effective Board of Directors is not expecting risk avoidance – it expects to be informed as to what risk we ***should*** take to meet business objectives and deliver returns on risk

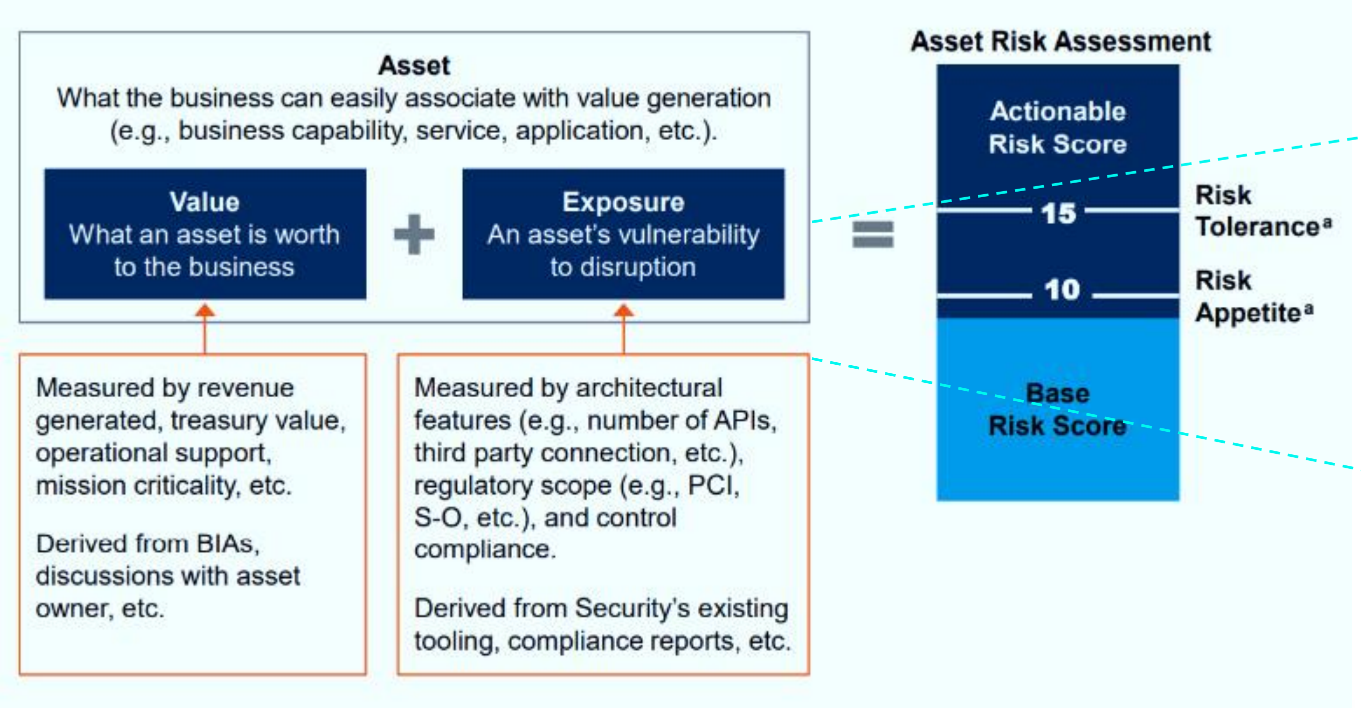
Agenda

- Qualitative versus Quantitative risk management
  – Why **Quantitative** Risk Management is a **pre-requisite** for the business

- Why managing solely based on **Annualized Loss Expectancy** and/or **Risk Reduction** is **not** Real Risk Management
- ***How*** to **build and scale** a quantitative cyber risk management capability for small and large organizations using automation and AI
- **How** to maximize the value of what is ***already known*** (or easily-knowable) in a Cyber Risk Quantification model
- Audience Questions and Discussion

Ground Cyber Risk Quantification in Asset Value, Not Loss Scenarios

“Grounds’ Rules” – Asset Value-based Cyber Risk Quantification Approach



Asset
What the business can easily associate with value generation (e.g., business capability, service, application, etc.).

Value
What an asset is worth to the business

+

Exposure
An asset’s vulnerability to disruption

Measured by revenue generated, treasury value, operational support, mission criticality, etc.

Derived from BIAs, discussions with asset owner, etc.

Measured by architectural features (e.g., number of APIs, third party connection, etc.), regulatory scope (e.g., PCI, S-O, etc.), and control compliance.

Derived from Security’s existing tooling, compliance reports, etc.

=

Asset Risk Assessment

Actionable Risk Score

15 — **Risk Tolerance**[a]

10 — **Risk Appetite**[a]

Base Risk Score

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.

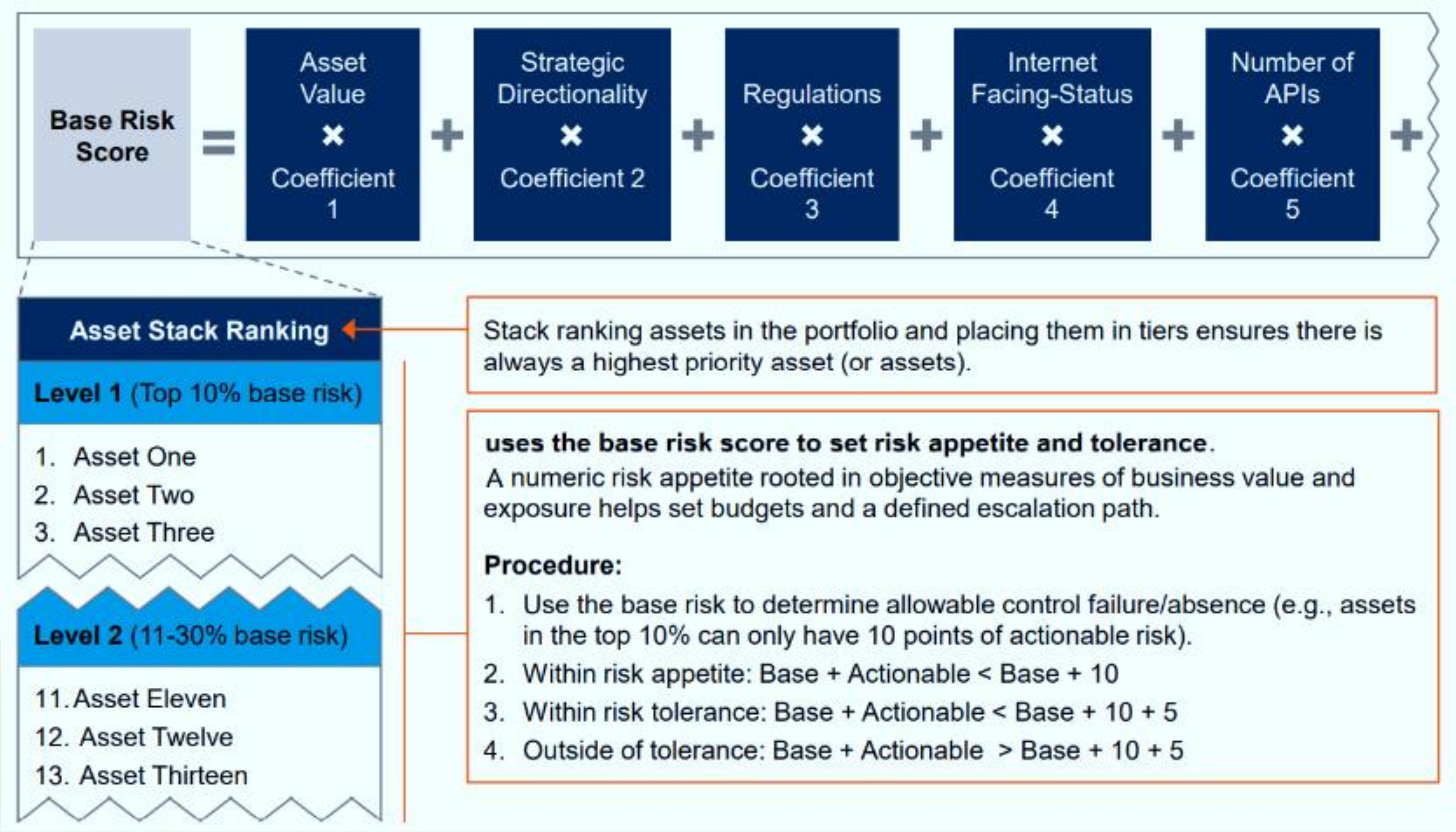
Grounds’ Rules for Cyber Risk Quantification:

“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.*

Ground Cyber Risk Quantification in Asset Value, Not Loss Scenarios

Asset Value Based Quantification



Base Risk Score = Asset Value × Coefficient 1 + Strategic Directionality × Coefficient 2 + Regulations × Coefficient 3 + Internet Facing-Status × Coefficient 4 + Number of APIs × Coefficient 5 +

Asset Stack Ranking

Level 1 (Top 10% base risk)

1. Asset One
2. Asset Two
3. Asset Three

Level 2 (11-30% base risk)

11. Asset Eleven
12. Asset Twelve
13. Asset Thirteen

Stack ranking assets in the portfolio and placing them in tiers ensures there is always a highest priority asset (or assets).

uses the base risk score to set risk appetite and tolerance.

A numeric risk appetite rooted in objective measures of business value and exposure helps set budgets and a defined escalation path.

Procedure:

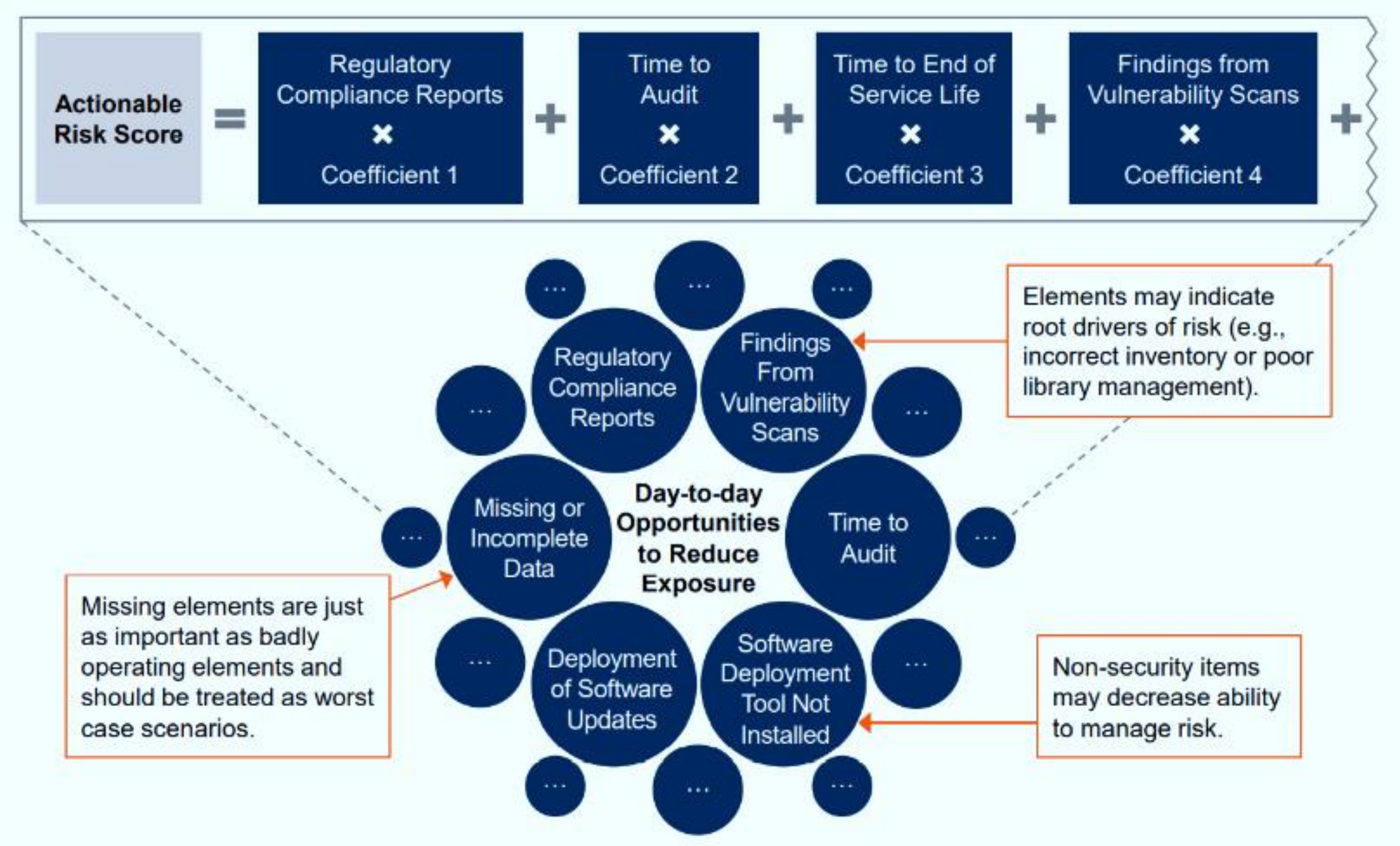
1. Use the base risk to determine allowable control failure/absence (e.g., assets in the top 10% can only have 10 points of actionable risk).
2. Within risk appetite: Base + Actionable < Base + 10
3. Within risk tolerance: Base + Actionable < Base + 10 + 5
4. Outside of tolerance: Base + Actionable > Base + 10 + 5

** Source: Adapted from Gartner. Case Study on Verizon and “Grounds’ Rules” method.*

**** illustrative data only***

Ground Cyber Risk Quantification in Asset Value, Not Loss Scenarios

Actionable Risk Quantification



Actionable Risk Score = Regulatory Compliance Reports × Coefficient 1 + Time to Audit × Coefficient 2 + Time to End of Service Life × Coefficient 3 + Findings from Vulnerability Scans × Coefficient 4 +

Day-to-day Opportunities to Reduce Exposure
Regulatory Compliance Reports
Findings From Vulnerability Scans
Missing or Incomplete Data
Time to Audit
Deployment of Software Updates
Software Deployment Tool Not Installed
…

Elements may indicate root drivers of risk (e.g., incorrect inventory or poor library management).

Missing elements are just as important as badly operating elements and should be treated as worst case scenarios.

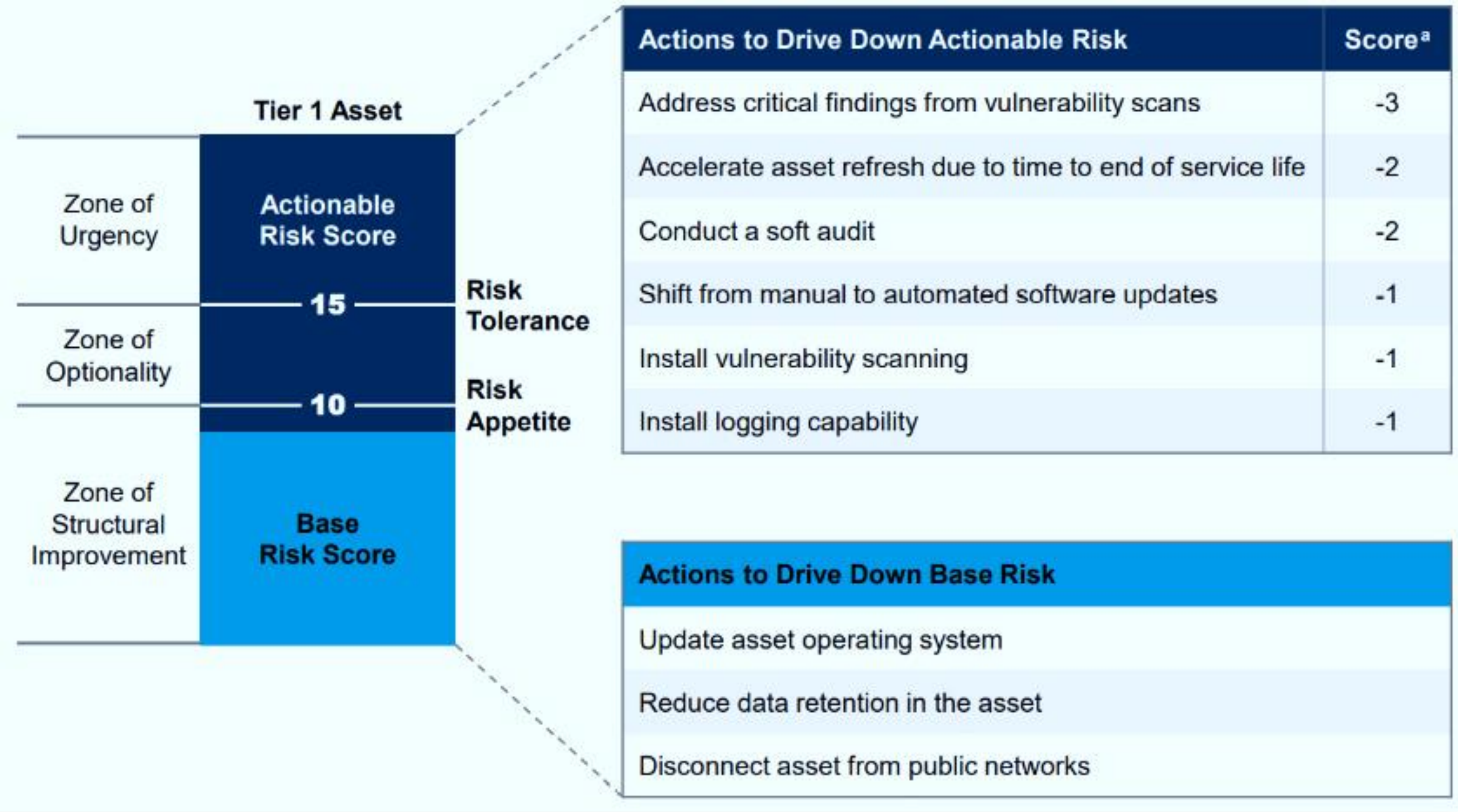
Non-security items may decrease ability to manage risk.

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

**** illustrative data only***

Ground Cyber Risk Quantification in Asset Value, Not Loss Scenarios

Link Action Options Explicitly to Exposure Reduction, not Loss 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

- Qualitative versus Quantitative risk management
  – Why **Quantitative** Risk Management is a **pre-requisite** for the business

- Why managing solely based on **Annualized Loss Expectancy** and/or **Risk Reduction** is **not** Real Risk Management
- ***How*** to **build and scale** a quantitative cyber risk management capability for small and large organizations using automation and AI
- **How** to maximize the value of what is ***already known*** (or easily-knowable) in a Cyber Risk Quantification model
- Audience Questions and Discussion

Ground Cyber Risk Quantification in Asset Value, Not Loss Scenarios

‘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

“Grounds’ Rules” Cyber Risk Quantification – Key Takeaways

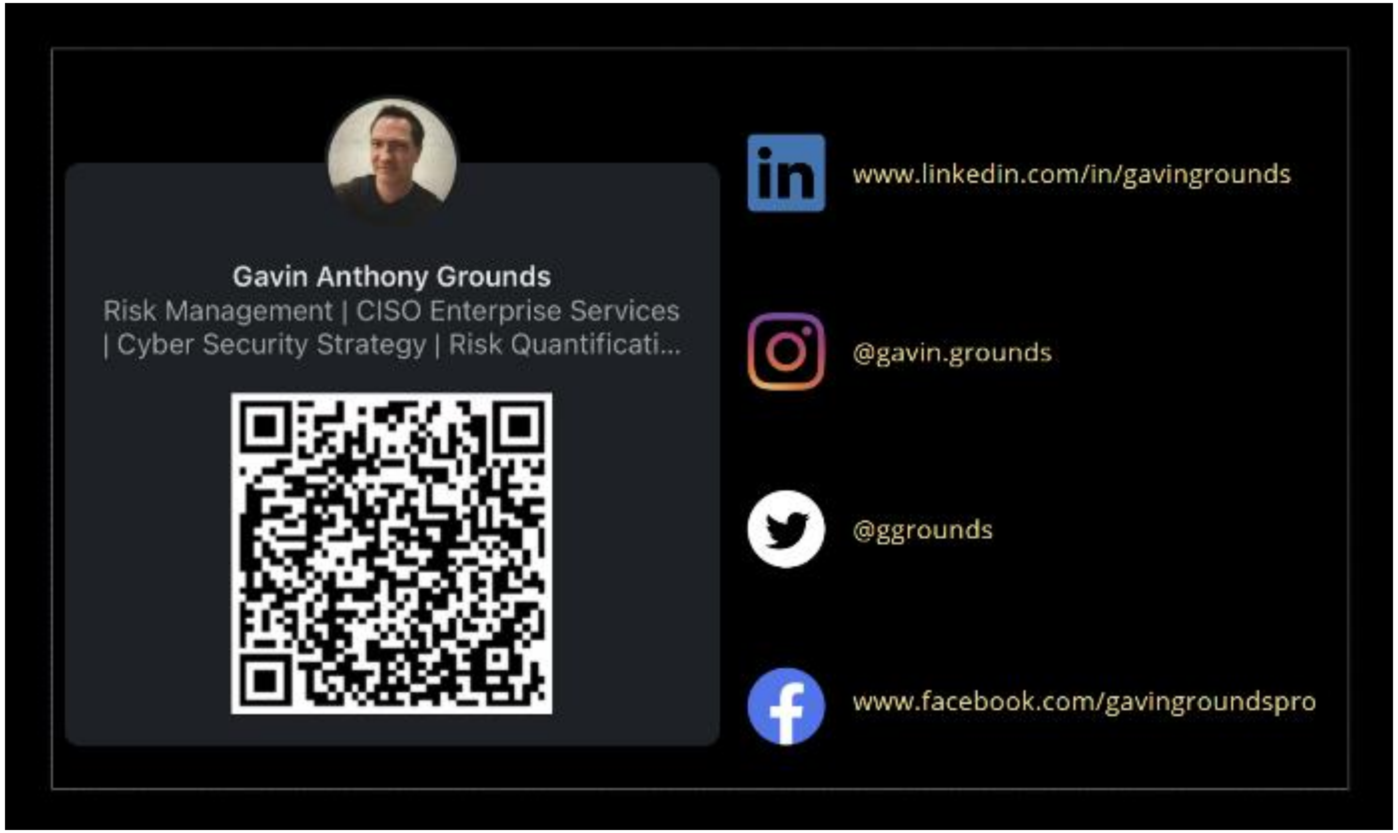
- Quantification of Cyber Security Risk is a **pre-requisite** for effective, business-oriented risk management
- Annualized Loss Expectancy and Risk Reduction strategies are not Risk Management
  - You cannot reduce Risk. You can exchange risks and you can reduce likelihood
- Monte Carlo Simulations 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)

Recommended Reading

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

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

Q & A



Gavin Anthony Grounds

Risk Management | CISO Enterprise Services | Cyber Security Strategy | Risk Quantificati...

in www.linkedin.com/in/gavingrounds

@gavin.grounds

@ggrounds

www.facebook.com/gavingroundspro