

An aerial photograph of a beach and high-rise buildings. The beach is on the left, with people and umbrellas. The ocean is a vibrant turquoise. To the right, several modern high-rise buildings with glass facades and balconies are visible. A large teal graphic overlay, consisting of a grid of lines, is positioned over the buildings and extends towards the beach. In the center, there is a white box with a black border containing the event information.

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**

Delivering Business Value through Risk Management, Compliance and Operational Excellence

Gavin A Grounds, Co-Founder & CEO Mercury Risk and Compliance

Grace Beason, Director Governance, Risk & Compliance, Guidewire Software;
Co-Founder Mercury Risk & Compliance



GRC

SUMMIT 2023

MIAMI, JUNE 14 & 15

Hosted by MetricStream

EXPERIENCE
the Power of Connection

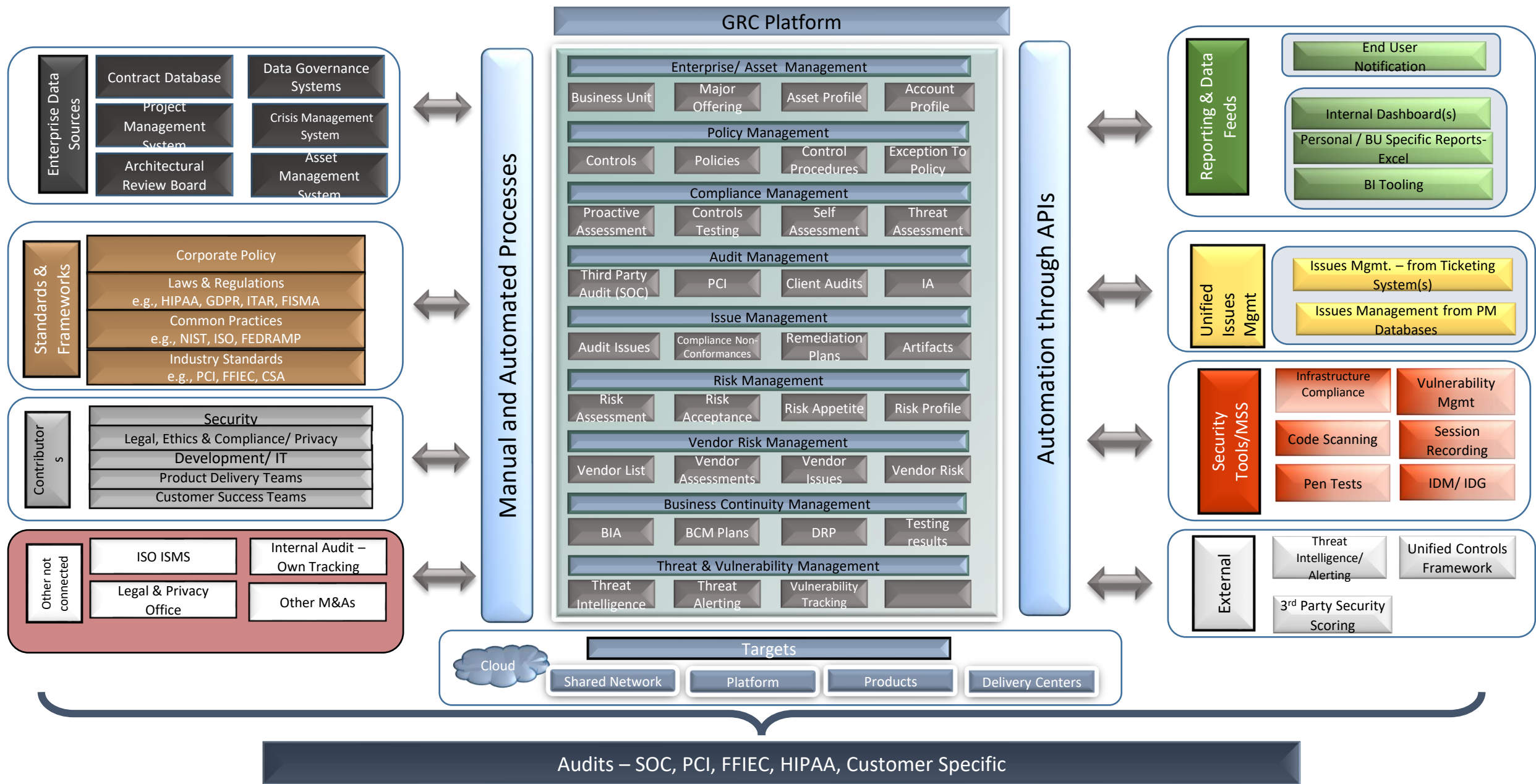
Automated Control Efficacy Testing (ACET)

Automated Control Efficacy Testing



- Internal & External Automation
 - Use of automated functions within a GRC tool
 - Use of API integration with security, risk and compliance tools
- Benefits
 - Scalable
 - Continuous or Near Real Time compliance
 - Value of Controls

There are controls that are **nice to have**
There are controls that you ***should have***
There are controls that you ***must have***





GRC

SUMMIT 2023

MIAMI, JUNE 14 & 15

Hosted by MetricStream

EXPERIENCE
the Power of Connection

Asset-Value Based Risk Quantification ("Grounds' Rules")

“Real” Risk Management – Case Study

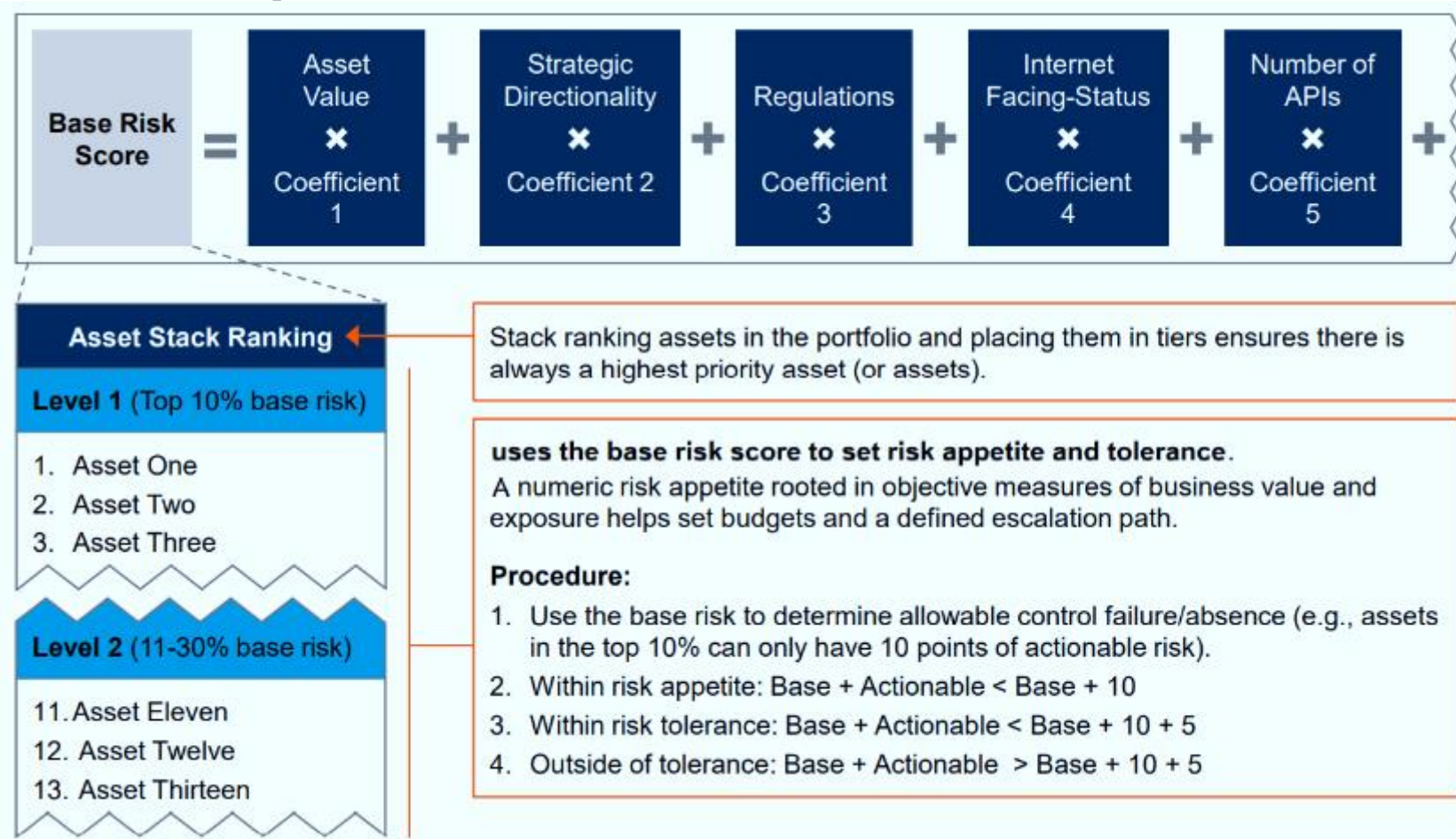
Darren



- 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 decreases **likelihood** of an accident which could result in death
- Slowing down increases **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

Ground Cyber Risk Quantification in Asset Value, Not Loss Scenarios (“Grounds’ Rules”)

Asset Value Based Quantification

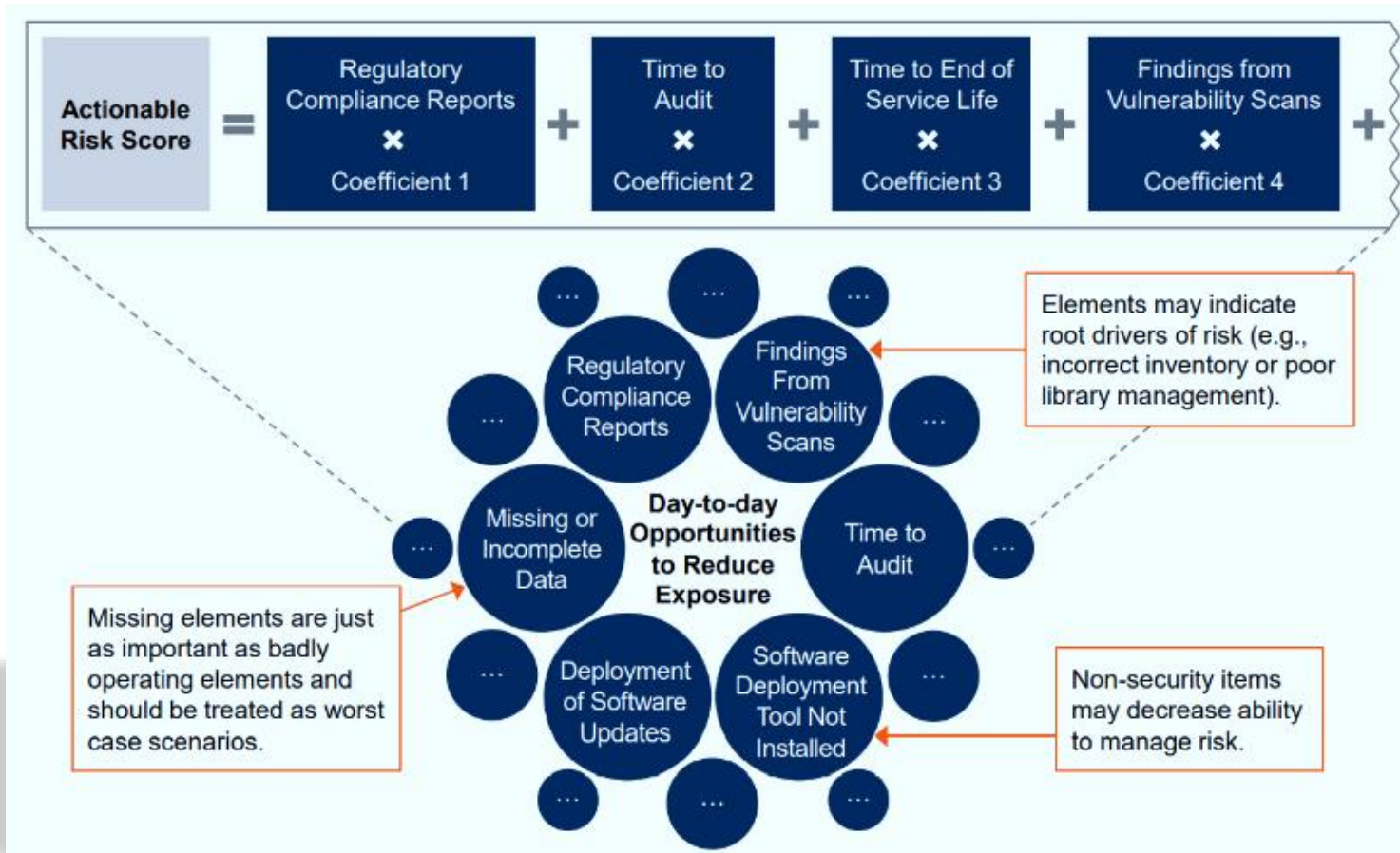


* Source: Adapted from Gartner. Case Study on Verizon and “Grounds’ Rules” method.

* illustrative data only

Ground Cyber Risk Quantification in Asset Value, Not Loss Scenarios

Actionable Risk Quantification



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

** illustrative data only*

Key Takeaways – Delivering Business Value

- **Integrate, integrate, integrate**
 - Re-keying data and “chasing updates” are examples of ***failure mode***
- **GRC is not solved by a single “tool”**
 - It is an ecosystem, or ***suite***, of functions, capabilities, tools and effective data flows
- **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)

An aerial photograph of a coastal city, likely Miami, featuring a wide sandy beach on the left, turquoise ocean waves, and a dense cluster of modern high-rise apartment buildings on the right. A semi-transparent green wireframe grid is overlaid on the scene, curving from the beach towards the buildings. In the center, a white box with a black border contains event information.

GRC

SUMMIT 2023

MIAMI, JUNE 14 & 15

Hosted by **MetricStream**

Q & A