

The background of the slide is a photograph of the Tower Bridge in London at night. The bridge's two towers are illuminated with warm lights, and the suspension cables are visible against the dark sky. The overall tone of the image is dark and atmospheric.

# GRC

SUMMIT 2022

LONDON, NOV 8-9

Hosted by MetricStream

## Delivering Business Value through Risk Management, Compliance and Operational Excellence

Gavin A Grounds, Sr. Director Security, Risk & Compliance, Meta

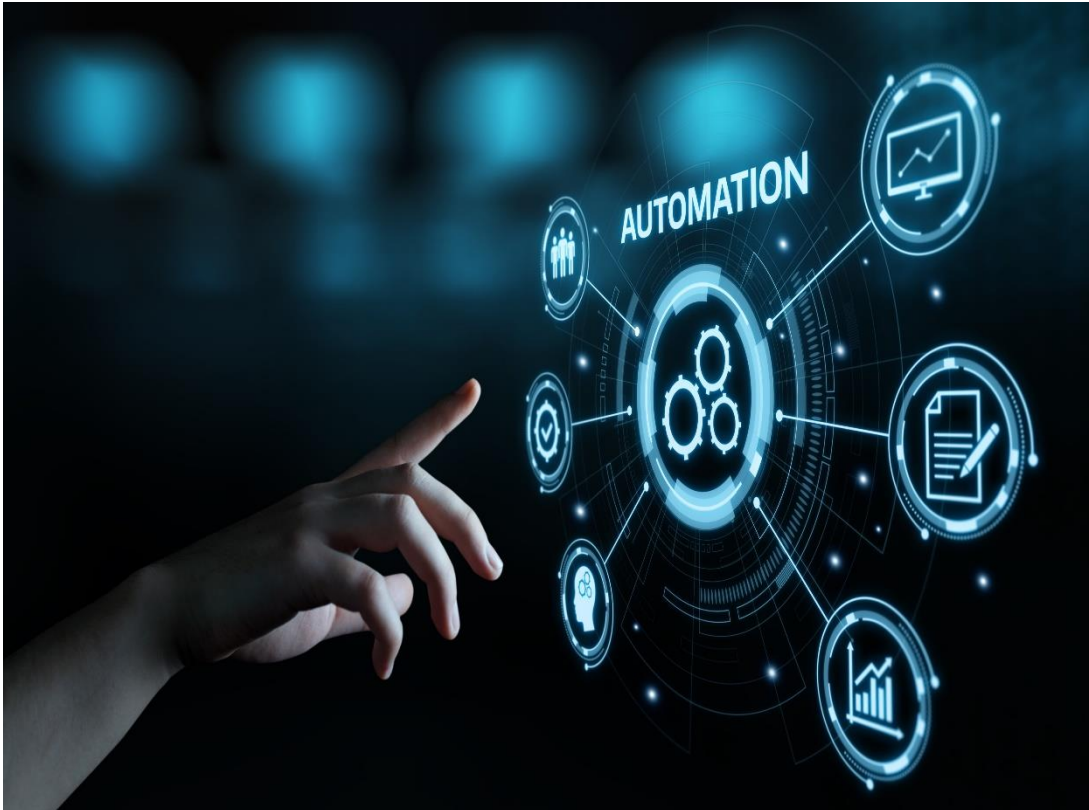
Grace Beason, Director Governance, Risk & Compliance, Guidewire Software

# Near Real Time Compliance Automation

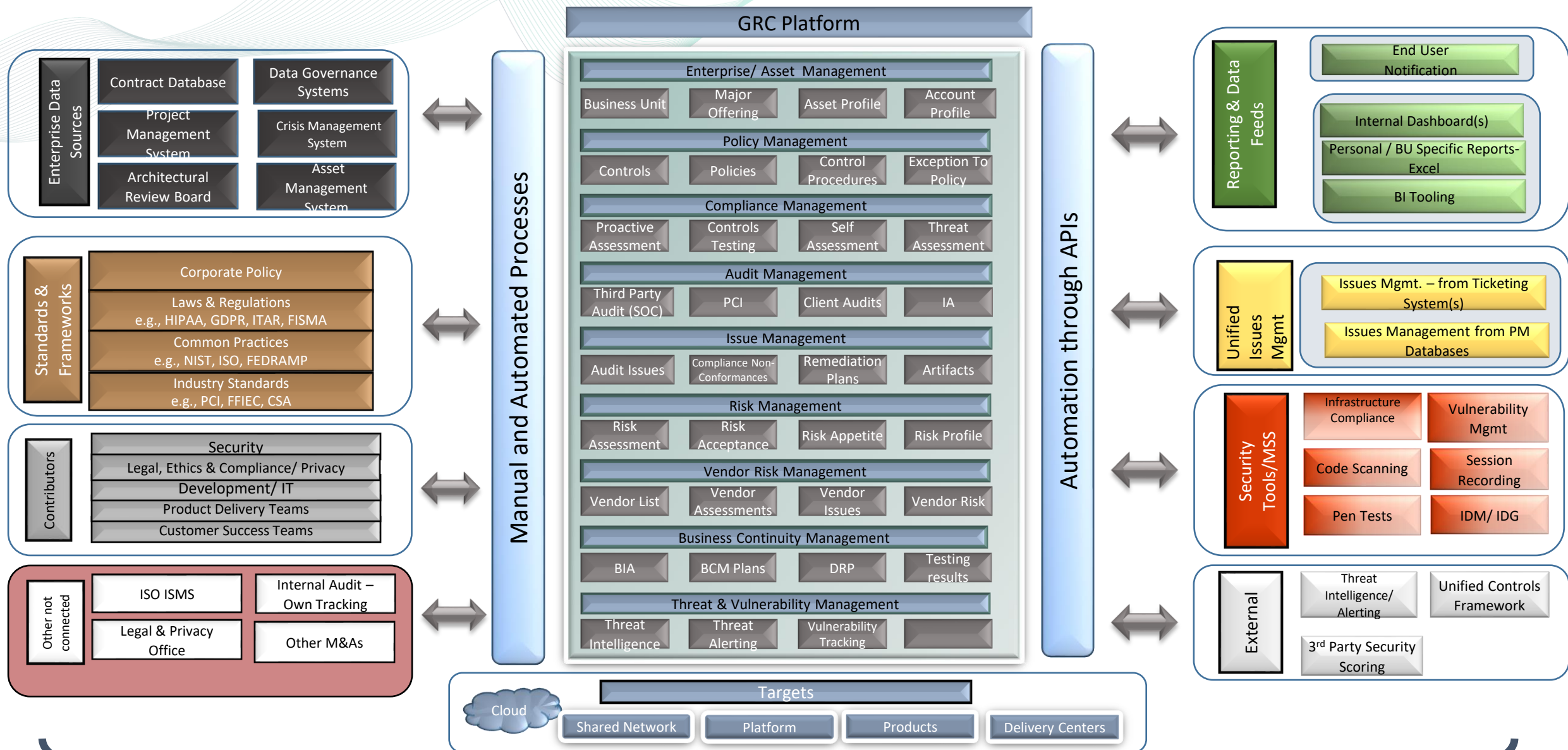




# Scale through Automation



- Internal Automation
  - Use of automated functions within a GRC tool
- External Automation
  - Use of API integration with security, risk and compliance tools
- Benefits
  - Scalable
  - Reduces risk of human error
  - ***Continuous / Near-real-time compliance*** vs. point in time compliance

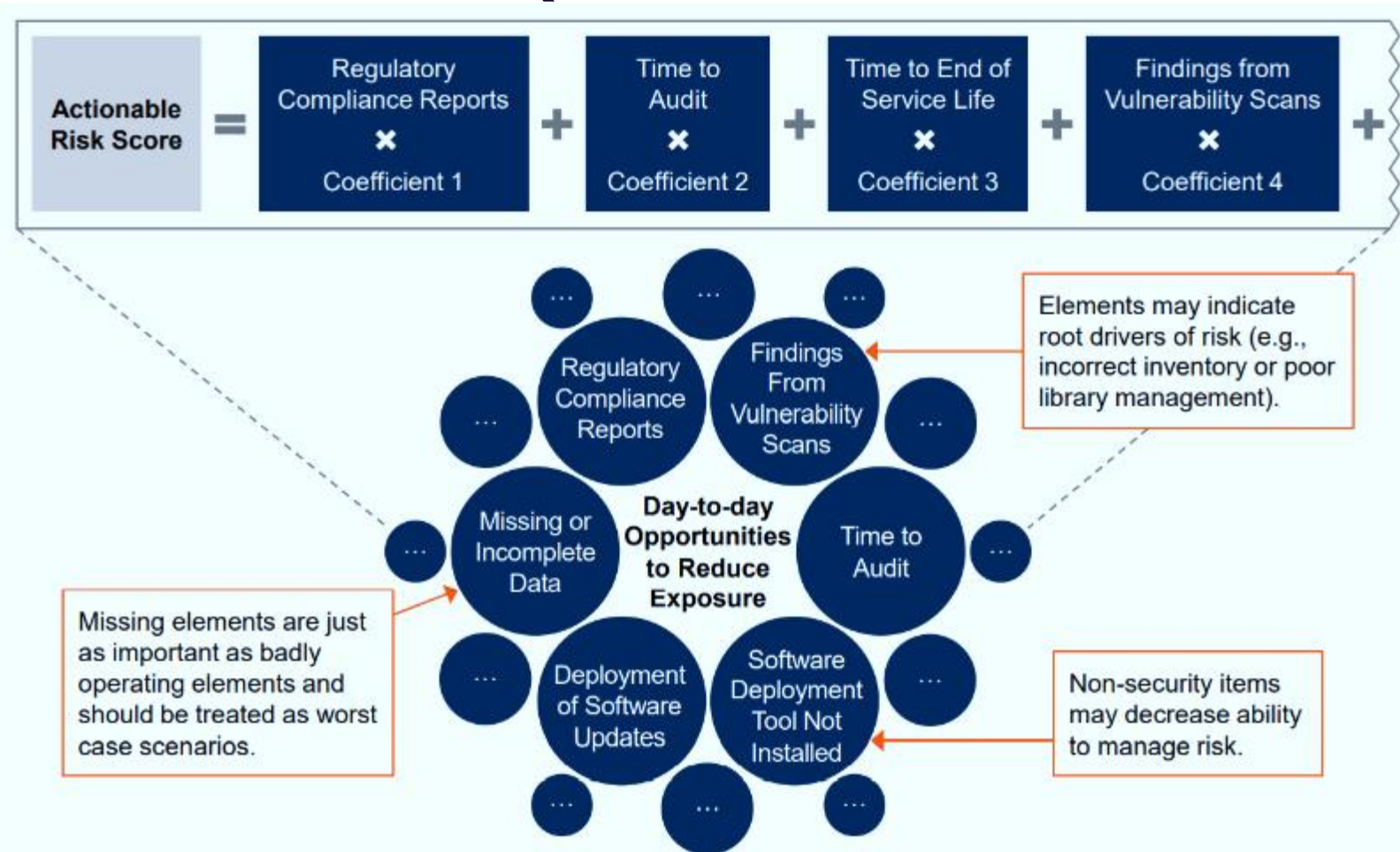


Audits – SOX, SOC, PCI, FFIEC, HIPAA, Customer Specific

# Comprehensive Cyber Risk Quantification

## – How to scale & deliver Business Value

### “Actionable-Risk” Quantification



- **Coefficients** are calibrated based on context
- Ensures that any given control is not overly-indexed
- **Likelihood** is inversely proportionate to measured control efficacy

\* 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

## “Base-Risk” Quantification



- **Likelihood**

is directly related to how “attractive” the asset, its exposure, and the efficacy of controls

*\* 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)

A night-time photograph of the Tower Bridge in London, illuminated with warm lights against a dark blue sky. The bridge's iconic towers and suspension cables are clearly visible.

# GRC

## SUMMIT 2022

LONDON, NOV 8-9

Hosted by **MetricStream**

### Q&A

Gavin A Grounds - [Gavin Anthony Grounds | LinkedIn](#)

Grace Beason - [Grace \(Spagnolo\) Beason | LinkedIn](#)

 **metricstream**  
thrive on risk™



# 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)