

The background of the slide is a photograph of the Tower Bridge in London at night. The bridge is illuminated with warm lights, and its two towers are prominent against the dark sky. The suspension cables and the bridge deck are also visible. In the foreground, there is a dark, silhouetted tree on the left and a metal railing along the riverbank.

# GRC

SUMMIT 2022


LONDON, NOV 8-9

Hosted by MetricStream

## How to Build and Scale a Business Relevant Risk and Compliance Capability

Grace Beason

Director Governance, Risk and Compliance  
Guidewire Software

- 
- Build and scale a fully integrated GRC program that drives financial value and operational efficiencies.
  - Establish partnership between GRC and business organizations to operate in a manner that optimizes risk in alignment with business outcomes.
  - Scale GRC through automation.



# Integrated GRC



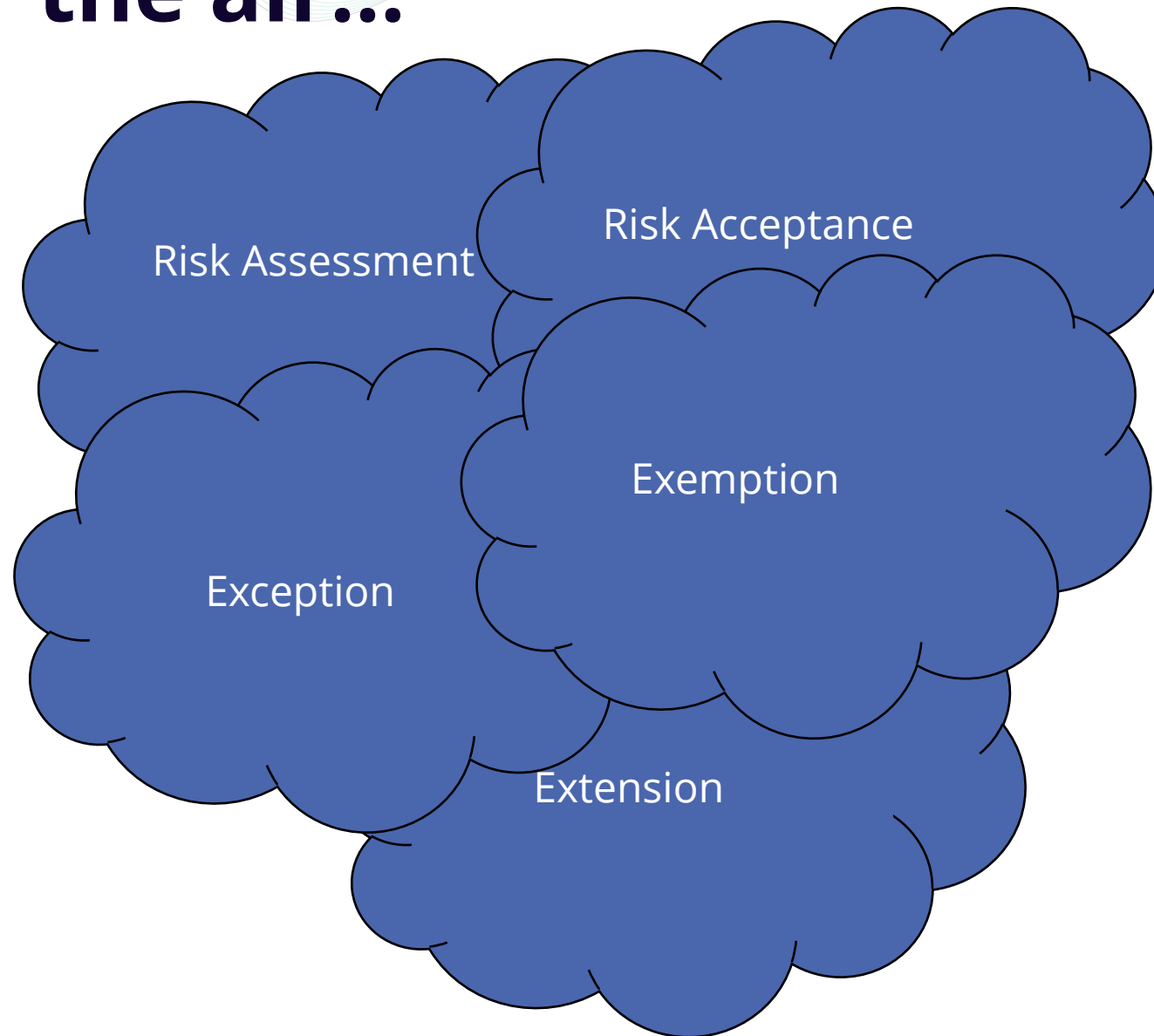
# It's not G or R or C"

**Integrated GRC** allows organizations to **optimize risk** while managing compliance in a manner that is based on **business context, business priorities** and as such drives risk-based business decisions.

- **Reduced fragmentation** among business units & eliminates **silos**
- Provides an **enterprise wide visibility** to compliance and risk postures.
- Allows the company to **apply a risk-based approach** to align cybersecurity with business objectives.
- Implements a **life-cycle compliance program** to ensure conformance with laws, regulations, industry, customer and corporate requirements.



# Let's clear the air...



# Integrated GRC



## Governance

- Define & Document Controls
- Training & Awareness
- Metrics & Reporting
- Governance of Issues & Risks

## Compliance

- Assess Effectiveness of Control
- Monitor Compliance
- Issue Management
- Policy Exception

## Risk

- Assessments
- Treatment
- Acceptance
- Register



# Partner With Business Owners



# Partnering with Business Owners

- **Common Challenges**

- Financial & Resource Allocation
- Competing Prioritization
- Complex Regulatory Requirements
- Audit Fatigue

- **Solutions**

- Increase Efficiency & Scale
- Increased Automation
- Agile Processes

- **GRC's Role**

- Role of Influence - Partner with stakeholders
- Use a top down / bottom-up approach
- USE DATA!!!!

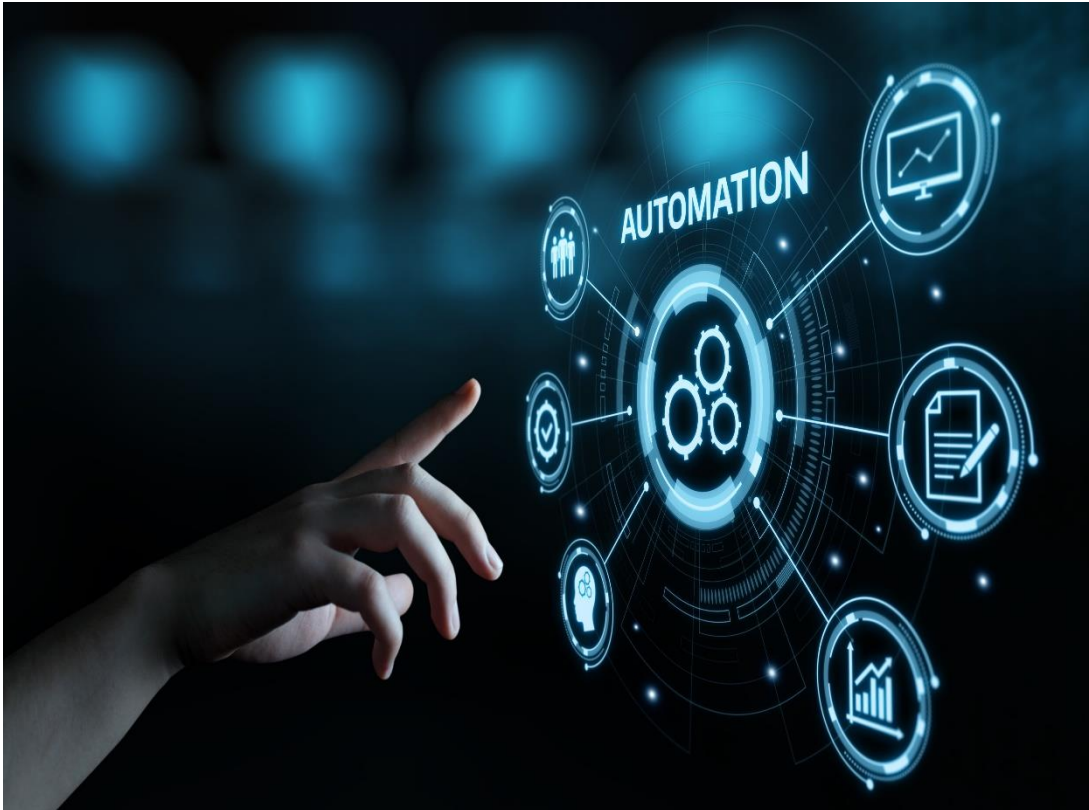




# Scale Through Automation

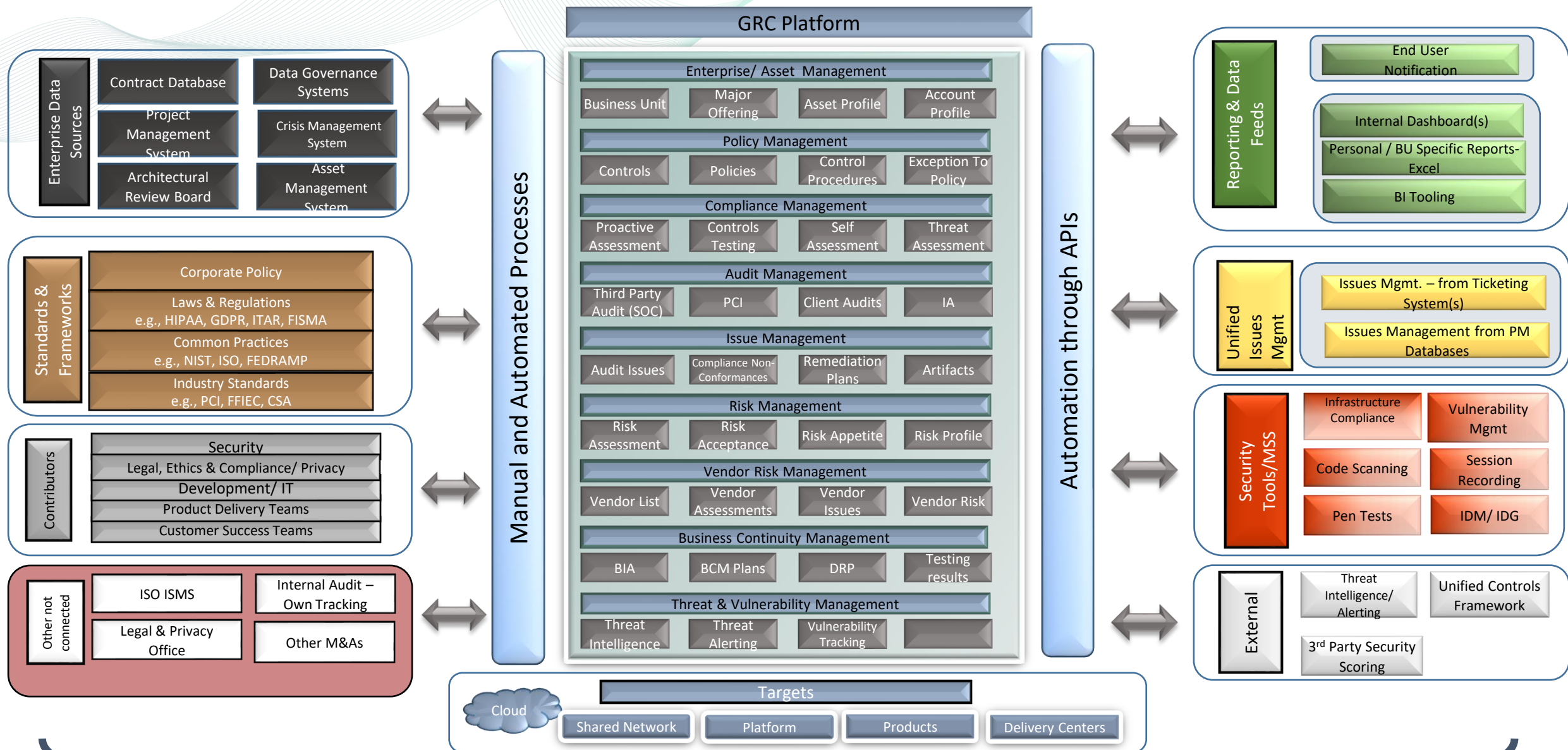


# Scale through Automation



- 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 compliance vs. point in time compliance





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



Q & A

