

The Resurrection of Governance, Risk & Compliance (GRC)

Steve Romero, IT Governance Evangelist
Romero Consulting

Governance, Risk & Compliance – G13



The background of the slide features a stylized illustration of the San Francisco skyline, including the Golden Gate Bridge and various city buildings, rendered in a muted color palette. Overlaid on this background is the "CyberSizeIT" logo, which consists of the word "CyberSizeIT" in a large, bold, red font with a white outline. The "C" is significantly larger and more stylized than the other letters.

WHAT YOU SIGNED UP FOR



The "CyberSizelT" logo is rendered in a large, stylized, red font with a white outline. The letters are slightly irregular, giving it a hand-drawn or artistic feel. In the background, there is a silhouette of the San Francisco skyline, including the Golden Gate Bridge and various city buildings, set against a light yellow and orange gradient sky.

The Resurrection of GRC

A story by Rick McElroy CISO ALLGRESS INC.

About the Author..



A black and white photograph of a man with a beard, wearing a white shirt and a dark vest, juggling four white eggs. He is looking down at the eggs with a focused expression. The background is dark. Several orange text labels are overlaid on the image, representing various IT and business concepts. The text is arranged around the man, with some labels positioned near the eggs he is juggling. The overall theme is 'In the Beginning...', suggesting the early stages of IT or business operations.

In the Beginning...

Technology

Money

Resources

Time

Firewalls

Visibility

Centralized Management

Viruses

And then there was GRC..



And then came...



We retooled...





And continue to lose...



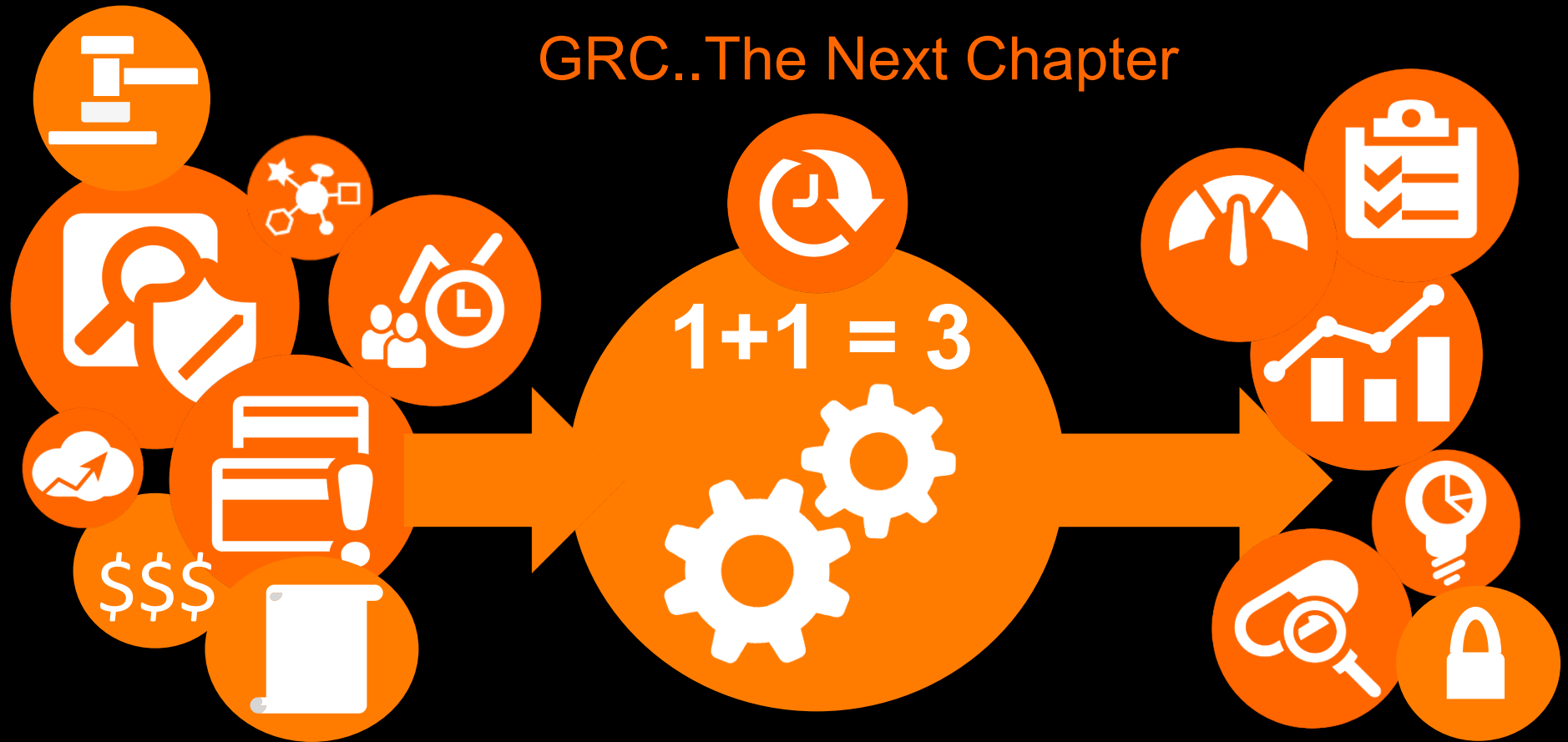
Obligatory Metrics Slide

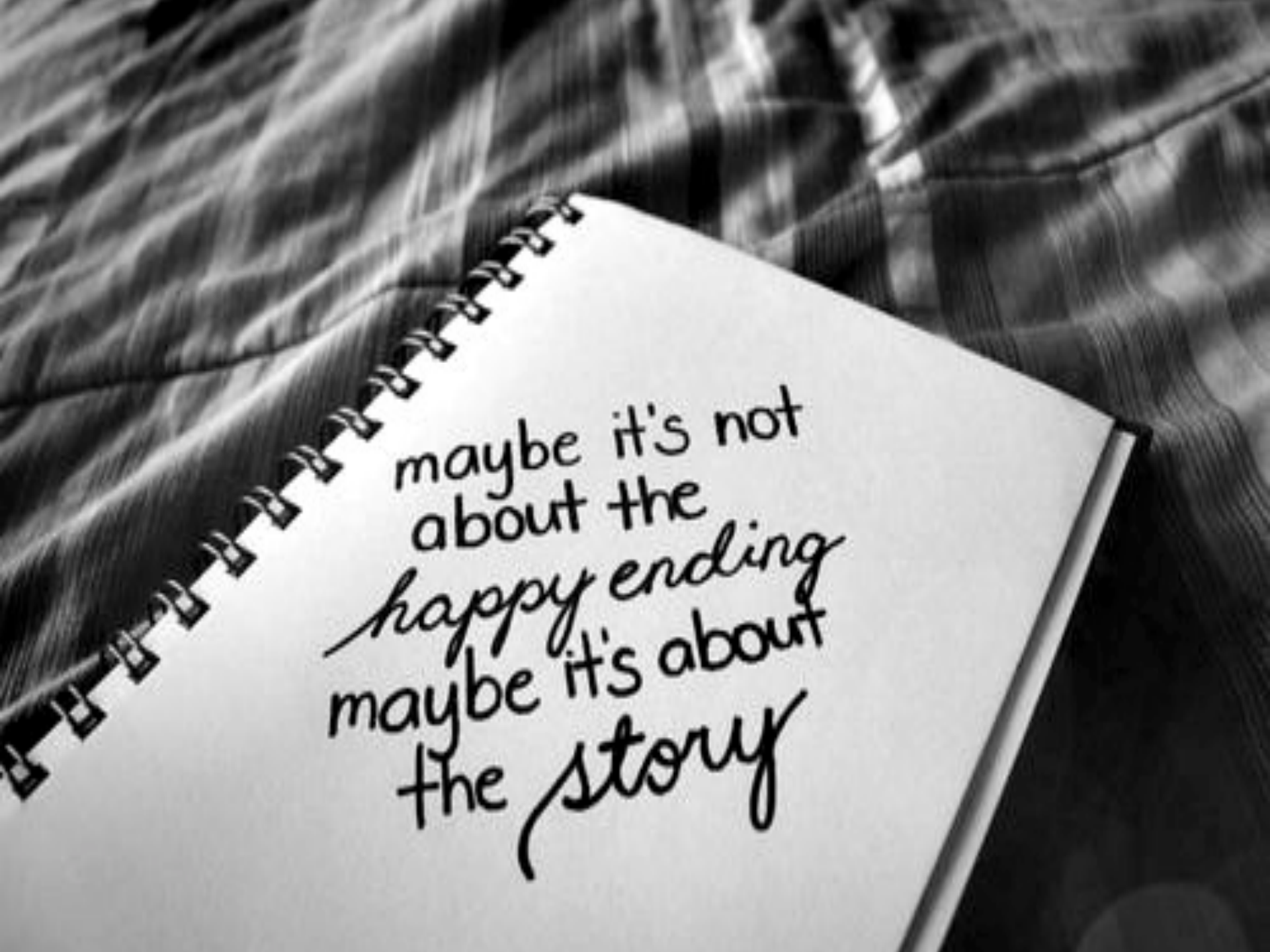
A black and white photograph of a weathered wooden signpost. The sign is a horizontal wooden plank with a pointed right end, mounted on a vertical post. The word "HOPE" is painted in white, bold, sans-serif capital letters on the left side of the plank. To the right of the text is a white arrow pointing towards the right tip of the plank. The background is a blurred, natural landscape.

HOPE

A new chapter is written

GRC..The Next Chapter



A black and white photograph of a spiral-bound notebook. The notebook is open, and the left page is visible, showing a spiral binding. The right page is blank and has handwritten text in a cursive script. The background is a plaid or checkered fabric. The lighting is soft, and the overall mood is contemplative.

maybe it's not
about the
happy ending
maybe it's about
the story

THE WORLD OF GRC



The "CyberSizelT" logo is rendered in a large, stylized, red font with a white outline. The letters are slightly irregular, giving it a hand-drawn or artistic feel. In the background, there is a silhouette of the San Francisco skyline, including the Golden Gate Bridge and various skyscrapers, set against a light yellow and orange gradient sky.

Google GRC

BWise
BUSINESS IN CONTROL

 Wolters Kluwer
Financial Services

ORACLE®


THE POWER TO KNOW.



SAP®

 HITEC

 software AG

2015
grc 2020

MetricStream

 R.sam

THE Network
A NAVEX Global Company

servicenow

GRC Definition

Governance, risk management, and compliance or GRC is the umbrella term covering an organization's approach across these three areas: Governance, risk management, and compliance

3 Pillars of GRC

Governance, Risk Management, and Compliance (GRC) are three pillars that work together for the purpose of assuring that an organization meets its objectives. ...

- Governance is the combination of processes established and executed by the board of directors that are reflected in the organization's structure and how it is managed and led toward achieving goals.
- Risk management is predicting and managing risks that could hinder the organization to achieve its objectives.
- Compliance with the company's policies and procedures, laws and regulations, strong and efficient governance is considered key to an organization's success.

Typical GRC

GRC is a discipline that aims to synchronize information and activity across governance, risk management and compliance in order to operate more efficiently, enable effective information sharing, more effectively report activities and avoid wasteful overlaps. Although interpreted differently in various organizations, GRC typically encompasses activities such as corporate governance, enterprise risk management (ERM) and corporate compliance with applicable laws and regulations.

Google GRC

BWise
BUSINESS IN CONTROL

 Wolters Kluwer
Financial Services

ORACLE®


THE POWER TO KNOW.



SAP®

 HITEC

 software AG

2015
grc 2020

MetricStream

 R.sam

THE Network
A NAVEX Global Company

servicenow

iiA ISACA GRC Conference



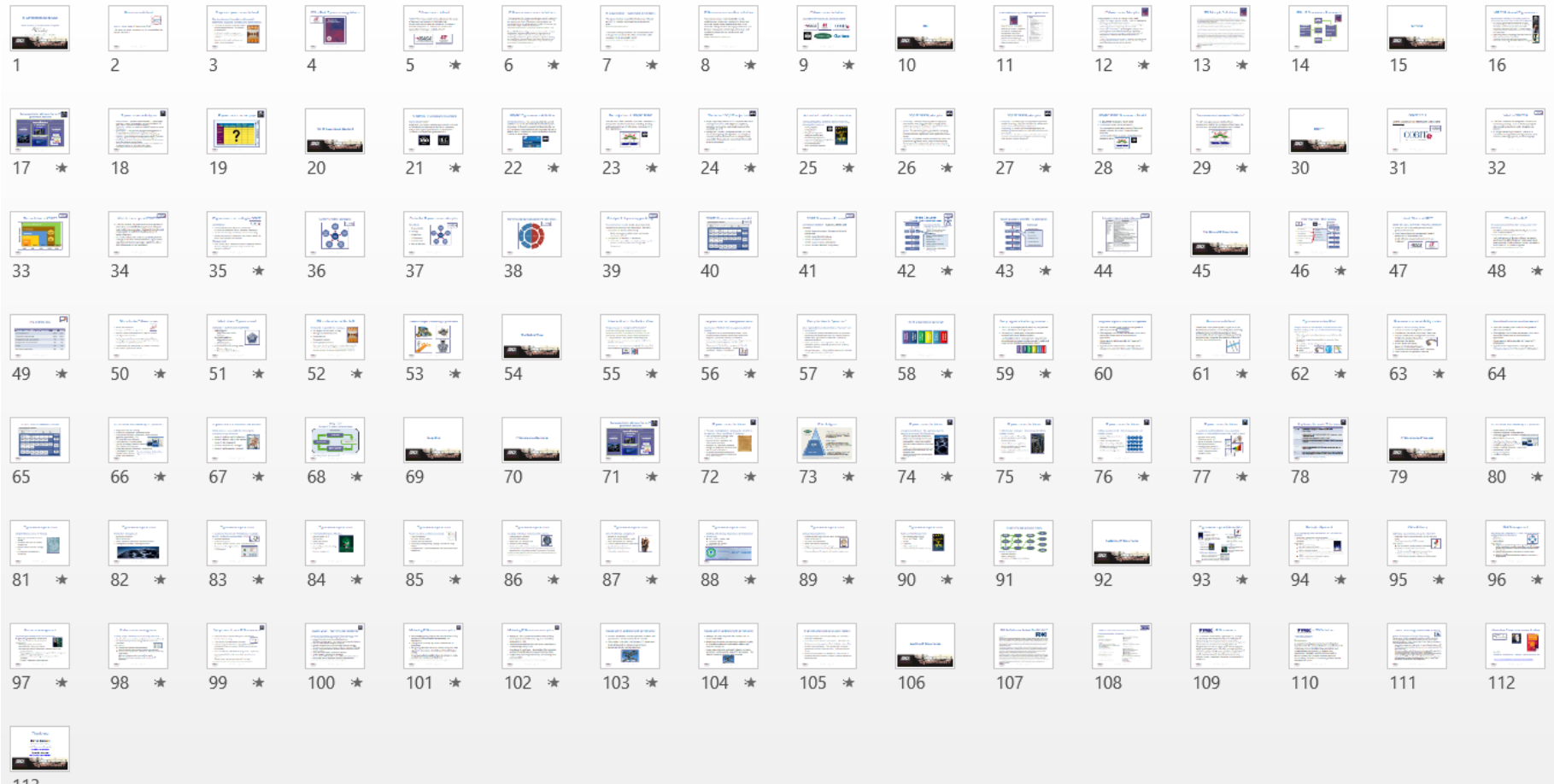
The banner features a green background with a series of white chevrons pointing right. On the left, the logos for 'The Institute of Internal Auditors' and 'ISACA' are displayed. On the right, the text '2015 GRC' is prominently shown in large blue letters, with 'an IIA & ISACA collaboration' in smaller text below it. Further down, the theme 'Where Governance and Risk Management Align for Impact' is written in white, followed by the dates 'August 17-19, 2015' and location 'Phoenix, Arizona, USA'. At the bottom right, a white button with blue text says 'REGISTER NOW' with a right-pointing arrow. To the left of the button, white text reads 'SAVE US\$200 when you register by June 5!'.

2015 GRC
an IIA & ISACA collaboration

Where Governance and Risk Management Align for Impact
August 17-19, 2015 | Phoenix, Arizona, USA

SAVE US\$200 when you register by June 5! [REGISTER NOW >](#)

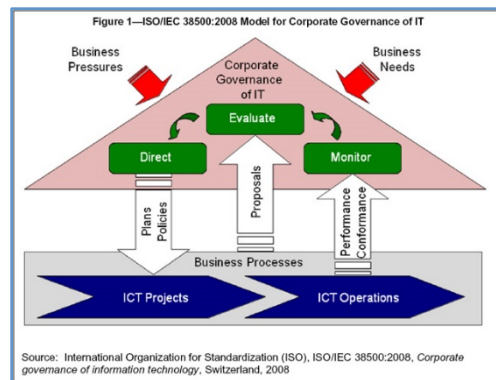
IT Governance

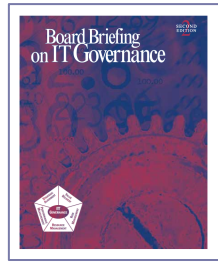


ISO/IEC 38500 Governance Model

IT is governed through 3 main tasks

- **Evaluate** the current and future use of IT.
- **Direct** preparation and implementation of plans and policies to ensure that use of IT meets business objectives.
- **Monitor** conformance to policies, and performance against the plans



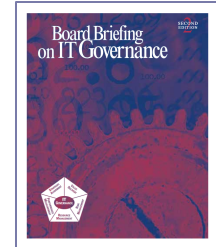
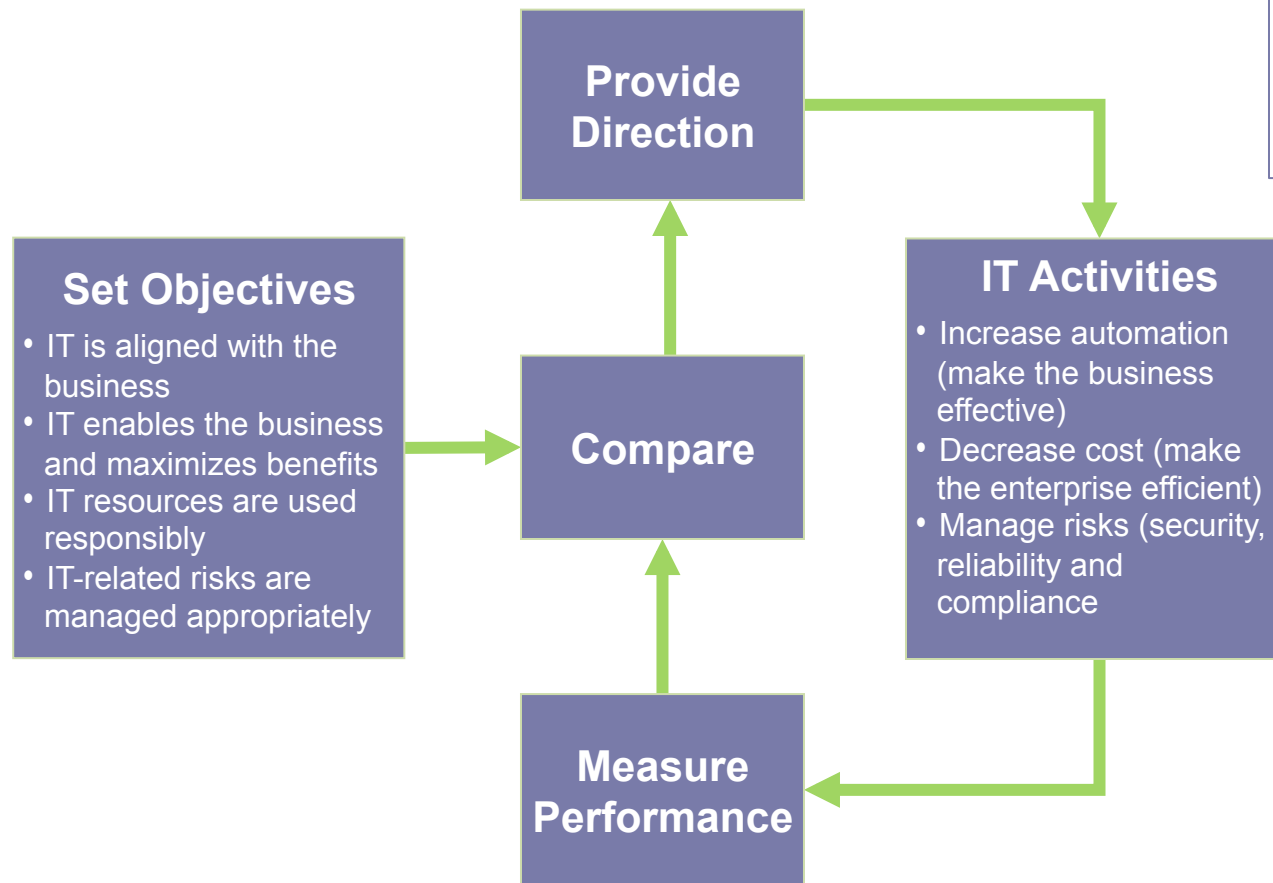


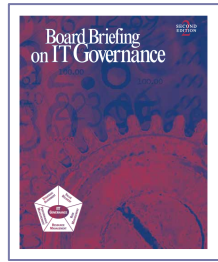
IT Governance Principles

The principles of ITG – according to ITGI, 1998

- **Ensure IT is aligned with the business** – focus on aligning with the business and collaborative solutions
- **Ensure IT delivers value to the business** – concentrating on optimizing expenses and proving the value of IT
- **Ensure IT risk is managed** – addressing the safeguard of IT assets, disaster recovery and continuity of operations
- **Ensure IT resources are managed** – realizing the optimal investment in, and proper management of, critical IT resources
- **Ensure IT performance is managed** – tracking and monitoring strategy implementation, project success, resource usage, process performance and service delivery

ITGI - IT Governance Framework





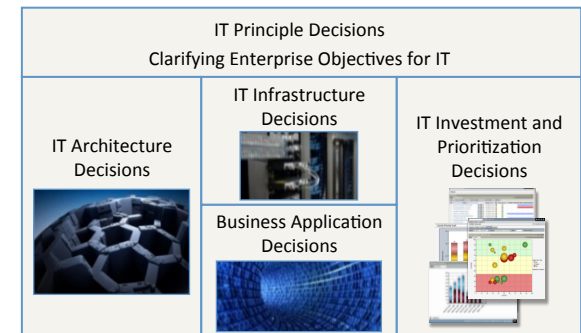
IT Governance Principles

The principles of ITG – according to ITGI, 1998

- **Ensure IT is aligned with the business** – focus on aligning with the business and collaborative solutions
- **Ensure IT delivers value to the business** – concentrating on optimizing expenses and proving the value of IT
- **Ensure IT risk is managed** – addressing the safeguard of IT assets, disaster recovery and continuity of operations
- **Ensure IT resources are managed** – realizing the optimal investment in, and proper management of, critical IT resources
- **Ensure IT performance is managed** – tracking and monitoring strategy implementation, project success, resource usage, process performance and service delivery

ITG decisions are enabled by ITG processes

- Integrated Business & IT Planning
- Architecture Management - Standards & Review
- IT Investment Assessment, Prioritization, Funding & Benefits Realization Accountability (PPM)
- IT Financial & Resource Allocation
- Project Execution & Decision-making
- Emerging Technology Evaluation & Adoption
- Client Relationship Management
- Building & Maintaining Applications & Infrastructure
- Provisioning of IT Services
- Strategic Sourcing Services
- Audit & Risk Management



*The other half of the Weill and Ross
IT governance mechanisms*

IT governance processes

Audit and Risk Management

- Risk modeling and assessment
- Partner with IT Audit – COBIT
- Security
- Compliance
- Policies & Standards
- Service continuity and disaster recovery



What is GRC to you?

- How do you define it?
- Why do you care?
- What are you trying to accomplish?
- Who else cares?
- What are *they* trying to accomplish?
- What are the **business** objectives?

Thank you

Steven Romero

IT Business Value Activist
and IT Governance Evangelist

steve@itgevangelist.com

Twitter @itgEvangelist

<http://www.itgevangelist.com/>

