



1

---

---

---

---

---

---

---

---

---

---



2

---

---

---

---

---

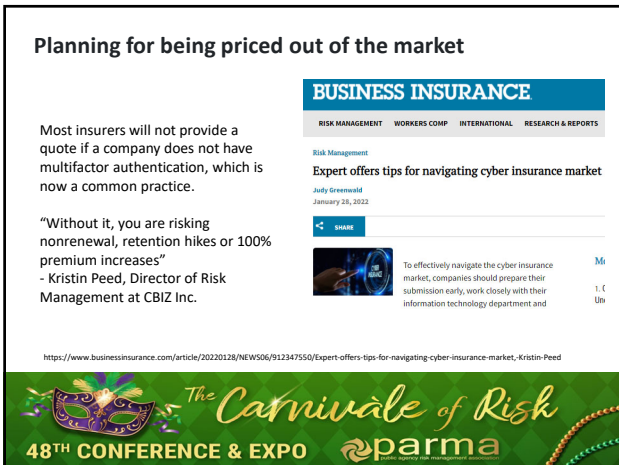
---

---

---

---

---



3

---

---

---

---

---

---

---

---

---

---





**IT risk is business risk**

**Risk is money**

**You don't know what you don't know**

7

---

---

---

---

---

---

---

---



**Cyber Risk Management Is:**

- Often reactionary
- Often focused only on IT security
- Lacks alignment with business objectives
- Check the box mentality
- Senior Executive are asking the wrong questions
- Compliance ≠ Security
- \$'s ≠ Security
- Extremely difficult to Quantify

8

---

---

---

---

---

---

---

---



**Donald E. Hester**  
@sobca

"The first step in the risk management process is to acknowledge the reality of risk. Denial is a common tactic that substitutes deliberate ignorance for thoughtful planning."  
-Charles Tremper

**"The Emperor does not share your optimistic appraisal of the situation."**

Darth Vader to Moff Jerjerrod, Return of the Jedi



9

---

---

---

---

---

---

---

---



**Gartner Research**

**8 Reasons More CEOs Will Be Fired Over Cybersecurity Incidents**

**Equifax CEO Rick Smith's Congressional Testimony**

**Gartner's Analysis:**

**"Equifax's CEO did not prioritize cybersecurity."**

**Summary**  
Gartner research shows that CEOs are increasingly being blamed and punished as a result of cybersecurity-related events — even more so than IT executives. CIOs concerned with IT risk must help CEOs achieve greater defensibility with key stakeholders.

<https://www.gartner.com/en/documents/3904673/8-reasons-more-ceos-will-be-fired-over-cybersecurity-inc>

10

---

---

---

---

---

---

---

---

---

---



**Business Decisions**

Business Decision makers are disconnected from the cyber realities.

Do not know that an incident can lead to serious harm.

This should keep executives up at night.

11

---

---

---

---

---

---

---

---

---

---



**What questions should management be asking IT?**

**What questions should the board/council be asking IT?**

12

---

---

---

---

---

---

---

---

---

---



*The Carnival of Risk*  
48<sup>TH</sup> CONFERENCE & EXPO **parma**  
public agency risk management association

Is the information and technology within your organization being used to generate its maximum value to stakeholders?

13

---

---

---

---

---

---

---

---



*The Carnival of Risk*  
48<sup>TH</sup> CONFERENCE & EXPO **parma**  
public agency risk management association

Is management ensuring that the appropriate capabilities are in place with sufficient resources to reach goals, mission, innovation and ultimately business transformation?

14

---

---

---

---

---

---

---

---



*The Carnival of Risk*  
48<sup>TH</sup> CONFERENCE & EXPO **parma**  
public agency risk management association

Is risk to both information and technology assets and the business strategies they support, being properly mitigated, in ways that match your unique risk profile?

15

---

---

---

---

---

---

---

---



**48<sup>TH</sup> CONFERENCE & EXPO** parma  
public agency risk management association

What comes to mind when you see the term "IT Governance"

16

---

---

---

---

---

---

---

---



**48<sup>TH</sup> CONFERENCE & EXPO** parma  
public agency risk management association

**Governance, Risk and Compliance (GRC)**

Some see governance as risk and compliance, however this is a narrow view, it is far more than just risk and compliance activities.

17

---

---

---

---

---

---

---

---



**48<sup>TH</sup> CONFERENCE & EXPO** parma  
public agency risk management association

**Gartner Glossary**

Gartner Glossary > | > It Governance (itg)

**It Governance (itg)**

Effective  
Efficient  
Enabling

**IT governance (ITG)** is defined as the processes that ensure the effective and efficient use of IT in enabling an organization to achieve its goals. IT demand governance (ITDG—what IT should work on) is the process by which organizations ensure the effective evaluation, selection, prioritization, and funding of competing IT investments; oversee their implementation; and extract (measurable) business benefits. ITDG is a business investment decision-making and oversight process, and it is a business management responsibility. IT supply-side governance (ITSG—how IT should do what it does) is concerned with ensuring that the IT organization operates in an effective, efficient and compliant fashion, and it is primarily a CIO responsibility.

<https://www.gartner.com/en/information-technology/glossary/it-governance>

18

---

---

---

---


---

---

---

---





**ISACA Definition**

Enterprise governance of information and technology (EGIT) is concerned with value delivery from digital transformation and the mitigation of business risk that results from digital transformation.

Ensure value is brought to the organization

Ensure risks are identified and addressed

<https://www.isaca.org/Pages/Glossary.aspx>

19

---

---

---

---

---

---

---

---



**COBIT 2019**

“EGIT...is exercised by the board that oversees the definition and implementation of processes, structures and relational mechanisms in the organization that enable both business and IT people to execute their responsibilities in support of business/IT alignment and the creation of business value from I&T-enabled business investments.”

© ISACA COBIT 2019

20

---

---

---

---

---

---

---

---



Organizational success depends on the ability of Information and Technology to enable achievement of business goals.

21

---

---

---

---

---

---

---

---



*The Carnival of Risk*  
48<sup>TH</sup> CONFERENCE & EXPO **parma**  
public agency risk management association

Effective IT governance helps ensure that IT supports business goals, maximizes business investment in IT, and appropriately manages IT-related risks and opportunities.

22

---

---

---

---

---

---

---

---



*The Carnival of Risk*  
48<sup>TH</sup> CONFERENCE & EXPO **parma**  
public agency risk management association

A right-sized governance program does more than manage performance — it creates value throughout your enterprise.

23

---

---

---

---

---

---

---

---



*The Carnival of Risk*  
48<sup>TH</sup> CONFERENCE & EXPO **parma**  
public agency risk management association

Governance is vital to get the most out of enterprise information and technology (I&T)

24

---

---

---

---

---

---

---

---





**The Carnival of Risk**  
48<sup>TH</sup> CONFERENCE & EXPO parma  
public agency risk management association

Important enough that governance gets visibility at the board or council level.

25

---

---

---

---

---

---

---

---



**The Carnival of Risk**  
48<sup>TH</sup> CONFERENCE & EXPO parma  
public agency risk management association

### Key Benefits of Governance

 <p>Ensure value is brought to the organization</p>	 <p>Ensure risks are identified and addressed</p>	
Benefits realization	Resource optimization	Risk optimization
 VALUE	 RESOURCE OPTIMIZATION	 RISK

**COBIT<sup>2019</sup>**

26

---

---

---

---

---

---

---

---



**The Carnival of Risk**  
48<sup>TH</sup> CONFERENCE & EXPO parma  
public agency risk management association

### How do you measure the value of information and technology?

Value as:  
Benefits Realization & Resource Optimization



Ensure value is brought to the organization

27

---

---

---

---

---

---

---

---



## Benefits Realization

- Creating value for the enterprise through I&T
- Maintaining & increasing value from existing I&T
- Eliminating what is not creating sufficient value
- Delivery of fit-for-purpose services and solutions
- Aligned directly with business values
- Measured to demonstrate impact and contribution

28

---

---

---

---

---

---

---

---



## Resource Optimization

- Appropriate capabilities are in place
- Appropriate & effective use of resources
- Integrated, economical IT infrastructure
- New technology is introduced as required
- Obsolete systems are updated or replaced
- Recognizes the importance of people
- Gain optimal value from data & information

29

---

---

---

---

---

---

---

---



## How do you measure the mitigation of risk related to information and technology?



30

---

---

---

---

---

---

---

---



## Risk Optimization

- Addressing the **business risk** associated w/ I&T
- Focuses on the **preservation of value**
- Integrated within enterprise risk management
- Ensure a focus on IT by the enterprise
- Measured showing the impact & contributions of optimizing I&T-related business risk on preserving value

31

---

---

---

---

---

---

---

---



## Without EGIT

- Worse in aligning business and I&T strategies
- Less likely to achieve their intended goals
- Less likely to realize value
- Higher IT-related costs for continuity
- Less innovation
- Less trust between IT and business

32

---

---

---

---

---

---

---

---




33

---

---

---

---

---

---

---

---



## Governance of Information & Technology

<p><b>CIO or IT Director</b> Information Technology Information Systems</p> <p style="text-align: center;">Ensure value is brought to the organization</p> <p style="text-align: center;"><small>Service and value</small></p>	<p><b>CISO or Cybersecurity</b> Governance, Risk &amp; Compliance</p> <p style="text-align: center;">Ensure risks are identified and addressed</p> <p style="text-align: center;"><small>Safety and security</small></p>
--	--

34

---

---

---

---

---

---

---

---

## The Role of the CISO

- Governance of I & T
- Cyber Risk
- IT Compliance
- IT Assessment / Audit
- Cybersecurity Awareness
- Related Policies

A CISO is the executive-level manager who directs strategy, operations and the budget for the protection of the enterprise information assets and manages that program.

35

---

---

---

---

---

---

---

---



## Benefits

- Increased alignment between security and business objectives
- Development of information security that is elastic, nimble, and flexible to the business
- Reduction in wasted efforts and resources, and improvement in efficiency of security and the organization as a whole
- Opportunity to identify new, secure innovations and technology
- True synergy between security and business stakeholders, where the goals of both groups are being met

36

---

---

---


---

---

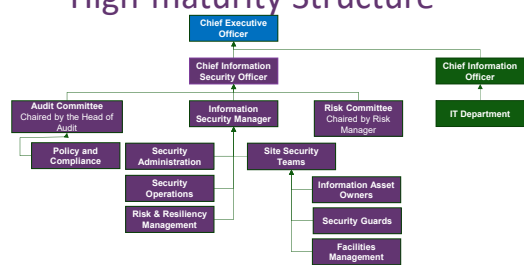
---

---


---



## High-maturity Structure



**48<sup>TH</sup> CONFERENCE & EXPO**  
February 27 – March 2, 2022



37

---

---

---

---

---

---

---

---

---

---

---

---



## Analyst Perspective

“ The days are gone when the security leader can stay at a desk and watch the perimeter. The rapidly increasing sophistication of technology, and of attackers, has changed the landscape so that a successful information security program must be elastic and nimble, and must be tailored to the organization’s specific needs.

The CISO is tasked with leading this modern security program, and this individual must truly be a Chief Officer, who has a finger on the pulses of the business and security processes at the same time. The modern, strategic CISO must be a master-of-all-trades.

A world-class CISO is a business enabler who finds creative ways for the business to take on innovative processes that provide a competitive advantage, and most importantly: to do so securely.

Cameron Smith  
Consulting Analyst, Security & Risk Practice  
Info-Tech Research Group

**48<sup>TH</sup> CONFERENCE & EXPO**  
February 27 – March 2, 2022



38

---

---

---

---

---

---

---


---

---

---

---

---



## City Council

“Only 26 percent of the CIOs believed that elected council members were either moderately or exceptionally aware of cybersecurity issues.”

- ICMA Cybersecurity Survey 2016

“...each city and town council should hold public discussions, at least annually, on their cybersecurity measures, which would also raise awareness among residents and local organizations on ways to improve cybersecurity.”

- Cyberattacks: A Growing Threat to Marin Government - Marin County Civil Grand Jury - May 11, 2020

39

---

---

---

---

---

---

---

---

---

---

---

---

## Complete Session Surveys on the App

Find the App, Click on Events, Click on Browse by Day, Click on the Specific Session, Click on Rate Event. See Below for Screen Shots.



---

---

---

---

---

---

---

---

---

---