TOP RISKS

# ON INFORMATION TECHNOLOGY

GANTULGA.B, CISA

IT AUDITOR

# AGENDA

- WHO AM I?
- TOP IT RISKS
- KEY TRENDS: CYBERSECURITY
- KEY TRENDS: DATA GOVERNANCE AND PRIVACY
- KEY TRENDS: REGULATORY COMPLIANCE
- IT RISK MANAGEMENT
- MATERIALS TO RELATED TO IT RISKS

# WHO AM I?

# WHO AM I

**Gantulga Batbayar**

IT AUDITOR

**CISA | CEH**

**COBIT | ITIL**

*I am an experienced IT Auditor with over 8+ years of experience in the fields of Audit, Cybersecurity, and IT Governance and management. I also worked for KhanBank, XacBank, and Unitel Group in Mongolia.*

## Professional Certifications

## CyberSecurity Awards

**2018 -** 2nd place in "Haruul Zangi" national cyber security competition - **n0m@d$ Team**

**2014** – 3rd place for Asia region in “Global Cyberlympics" online cyber security competition - **n0m@d$ Team**

**2014** - 1st place in "Haruul Zangi" national cyber security competition - **n0m@d$ Team**

**2013** – 3rd place for Asia region in "Global Cyberlympics" online cyber security competition - **n0m@d$ Team**

**2013** - 1st place in "Haruul Zangi" national cyber security competition - **n0m@d$ Team**

# Haruul Zangi – n0m@d$ Team

**2013 - 1st** place - **n0m@d$ Team**


**2014 - 1st** place - **n0m@d$ Team**


**2018 – 2nd** place - **n0m@d$ Team**





# TOP IT 10 RISKS

# SURVEY OBJECTIVE AND APPROACH

ISACA and Protiviti recently recently released the results of the 10th Annual IT Audit Technology Risks survey. Results of this global survey reveal cybersecurity, privacy, data and regulatory compliance are top-of-mind concerns.

# GLOBAL TOP 10 RISKS

2022 results are reasonably consistent with 2021

| Today's Top Technology Risks | 2022 | 2021 |
|---|---|---|
| Cyber breach | 1 | 1 |
| Manage security incidents | 2 | 5 |
| Privacy | 3 | 2 |
| Monitor regulatory compliance | 4 | 3 |
| Access risk | 5 | 4 |
| Data integrity | 6 | - |
| Disaster recovery | 7 | 6 |
| Data governance | 8 | 7 |
| Third-party risk | 9 | 8 |
| Monitor/audit IT, legal and regulatory compliance | 10 | - |

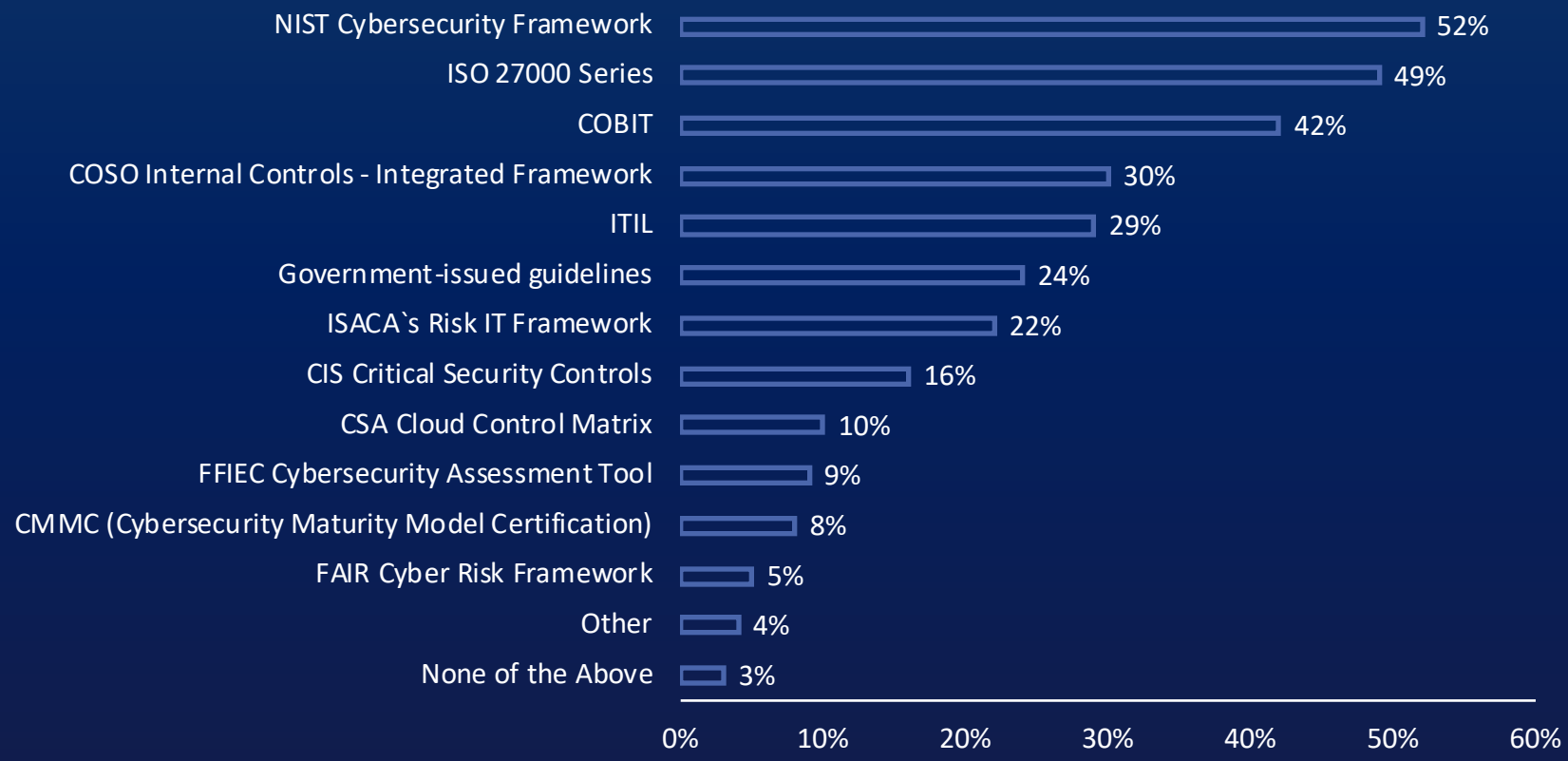
# INDUSTRY COMPARISON

# INDUSTRY RESULTS

| Rank | Financial Services | Public Sector | Energy and Utilities | Healthcare | Technology, Media and Telecommunications | Consumer Packaged Goods/Retail | Manufacturing and Distribution |
|---|---|---|---|---|---|---|---|
| 1 | Cyber breach | Cyber breach | Cyber breach | Cyber breach | Cyber breach | Cyber breach | Cyber breach |
| 2 | Monitor regulatory compliance | Manage security incidents | Manage security incidents | Privacy | Manage security incidents | Privacy | Manage security incidents |
| 3 | Manage security incidents | Privacy | Monitor regulatory compliance | Manage security incidents | Privacy | Access risk | Access risk |
| 4 | Privacy | Access risk | Access risk | Third-party risk | Monitor regulatory compliance | Manage security incidents | Privacy |
| 5 | Access risk | Data integrity | Third-party risk | Monitor regulatory compliance | Access risk | Third-party risk | Disaster recovery |
| 6 | Data integrity | Monitor regulatory compliance | Data governance | Access risk | Data integrity | Major projects | Data governance |
| 7 | Disaster recovery | Disaster recovery | Disaster recovery | Disaster recovery | Data governance | Data governance | Data integrity |
| 8 | Third-party risk | Data governance | Manage service losses or disruptions | Cloud strategy and adoption | Disaster recovery | Disaster recovery | Third-party |
| 9 | Data governance | Manage employee training and awareness | Data integrity | Monitor/ audit IT, legal, and regulatory compliance | Manage service losses or disruptions | Data integrity | Monitor regulatory compliance |
| 10 | Monitor/ audit IT, legal, and regulatory compliance | Manage service losses or disruptions | Monitor/ audit IT, legal, and regulatory compliance | Data integrity | Monitor/ audit IT, legal, and regulatory compliance | Cloud strategy and adoption | Manage services losses or disruptions |

# INDUSTRY FRAMEWORKS

Identifying and assessing technology risks



# KEY TREND: CYBERSECURITY

# TRENDS IN CYBERSECURITY

1 **Cloud**
The use of cloud has increased, necessitating the need for security measures to be put in place to avoid a data breach.

2 **Remote Working**
During remote working, an organization must identify areas of weakness that can cause vulnerability to threats while shifting to a remote workforce.

3 **Connected Devices**
Connected devices are increasingly connecting our physical world to the cyber realm. Up to 1 trillion connected devices are expected to be connected by 2025.

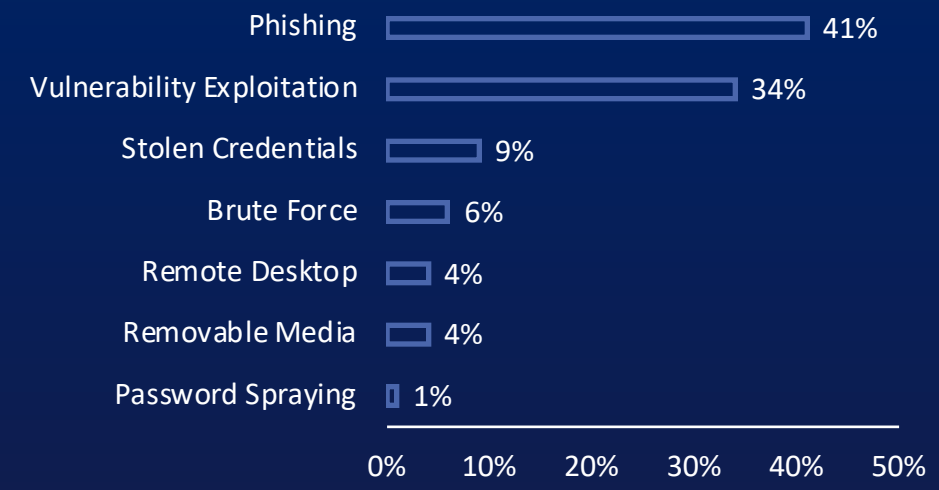
4 **Security Monitoring and Visibility**
Visibility of security tools and the ability to quickly detect and respond to potential security incidents is paramount in addressing today`s threats.

5 **Insider Threats**
Insider data breaches are on the rise, and companies should have the proper tools and systems in place to detect them.

6 **Patch management**
Organizations trying to proactively manage risks associated with security vulnerabilities require mature patch management programs.

7 **Identity and Access Management**
Identity is a core security control that is gaining greater significance as more of today`s modern IT environment rely on identify as the main security control.

**What Tactics were Used in a Breach (Actions)**




***Source:*** *IBM Security X-Force Threat Intelligence Index 2022 Full Report*

# KEY TREND:
# DATA GOVERNANCE AND PRIVACY

# TRENDS IN DATA GOVERNANCE AND DATA PRIVACY

1 **Third Party Vendors**
There is a growing reliance on third party vendors, which places greater importance on the design on operating effectiveness of vendor oversight and related data security controls.

2 **Data Privacy Regulations**
Further enactment of data privacy regulations around the world is making it more important to 'know your data' to maintain compliance and reduce regulatory fines.

3 **Talent and Retention Challenges**
55% of organizations are experiencing technical privacy staffing shortages, forcing most organizations to solicit external assistance.

## Considerations through the Data Lifecycle


*Source: ISACA 2022 State of Privacy Survey*

# KEY TREND:
# REGULATORY COMPLIANCE

# TRENDS IN IT REGULATOTY COMPLIANCE

## 1 New & Emerging Global Data Privacy Laws

Data protection and privacy regulations have emerged globally forcing institutions to remain vigilant and respond to avoid regulatory fines.

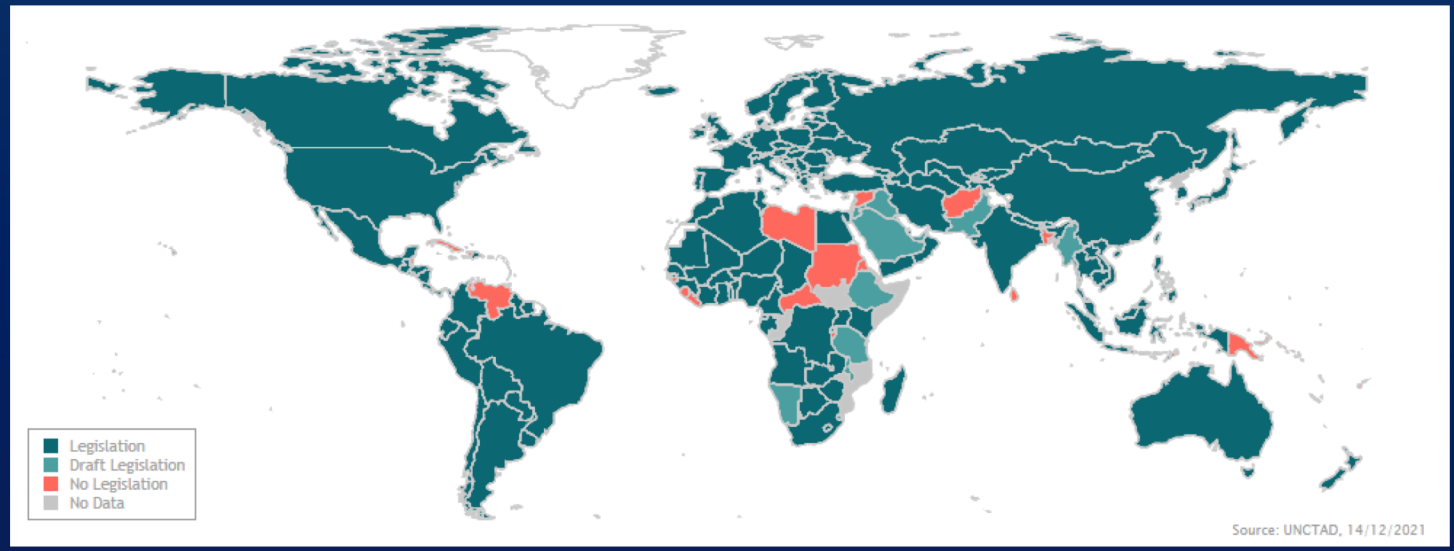
## 2 Data Privacy Regulations

In response to intensifying cyberattacks, the US has categorized more as “critical infrastructure” and additional organizations are subject to more stringent cybersecurity requirements.

## 3 Economic Sanctions

Unprecedented economic sanctions require organizations to better understand where business is conducted, including that of third parties and supply chains.

Data Protection and Privacy Legislation Worldwide (December 2021)

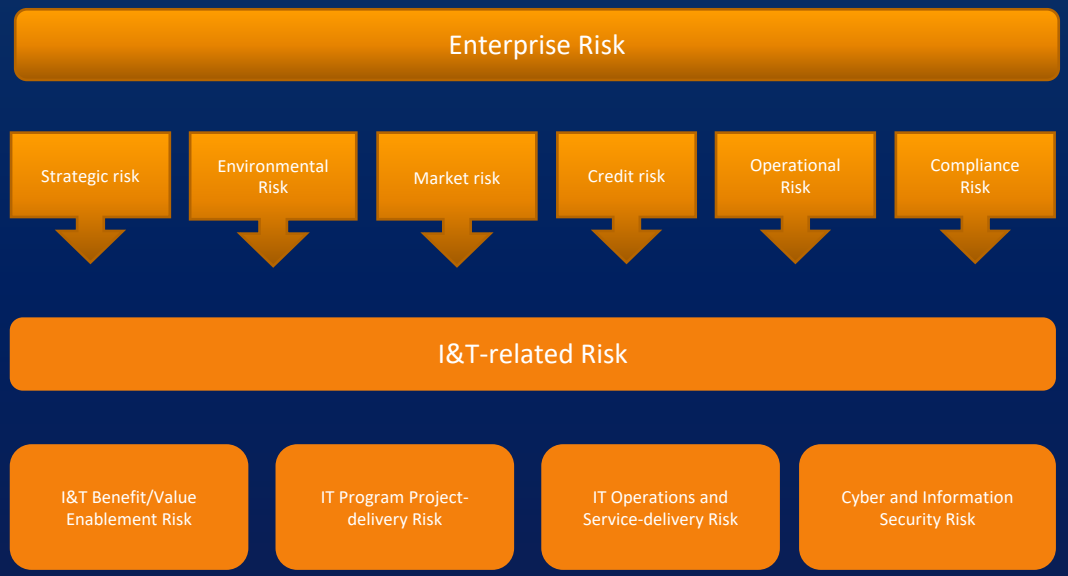



| 71% | 9% | 15% | 5% |
|---|---|---|---|
| Countries With Legislation | Countries With Draft Legislation | Countries With No Legislation | Countries With No Research data |

***Source:*** *https://unctad.org/page/data-protection-and-privacy-legislation-worldwide*

# IT RISK MANAGEMENT

## Scope of I&T-related Risk Relative to Other Major Categories of Risk




## Principles of Risk Management

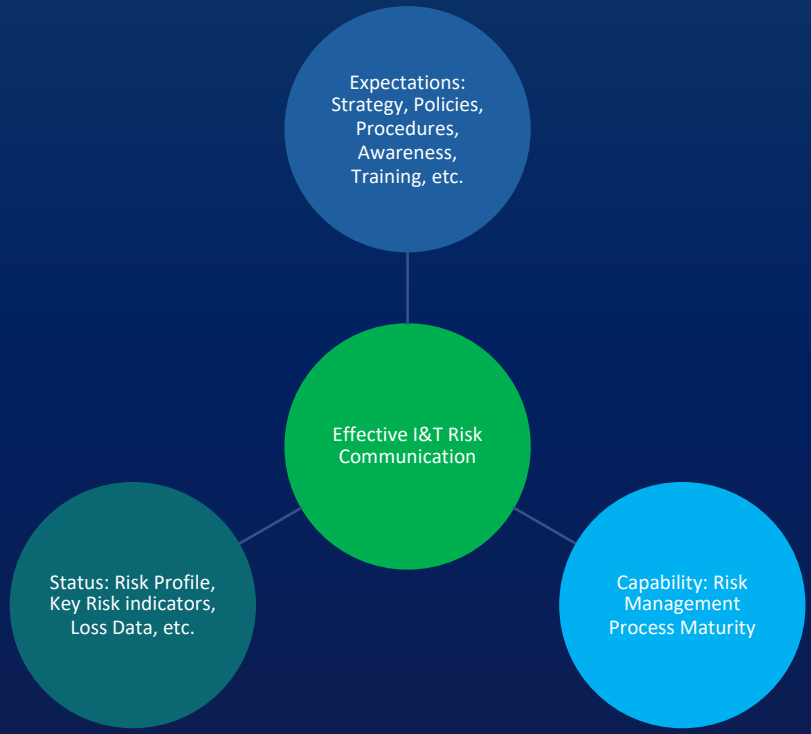

*Source: ISACA IT Risk Framework*

# Alignment of I&T-related Risk Management Principles with COBIT Objectives EDM03 and APO12


*Source: ISACA IT Risk Framework*

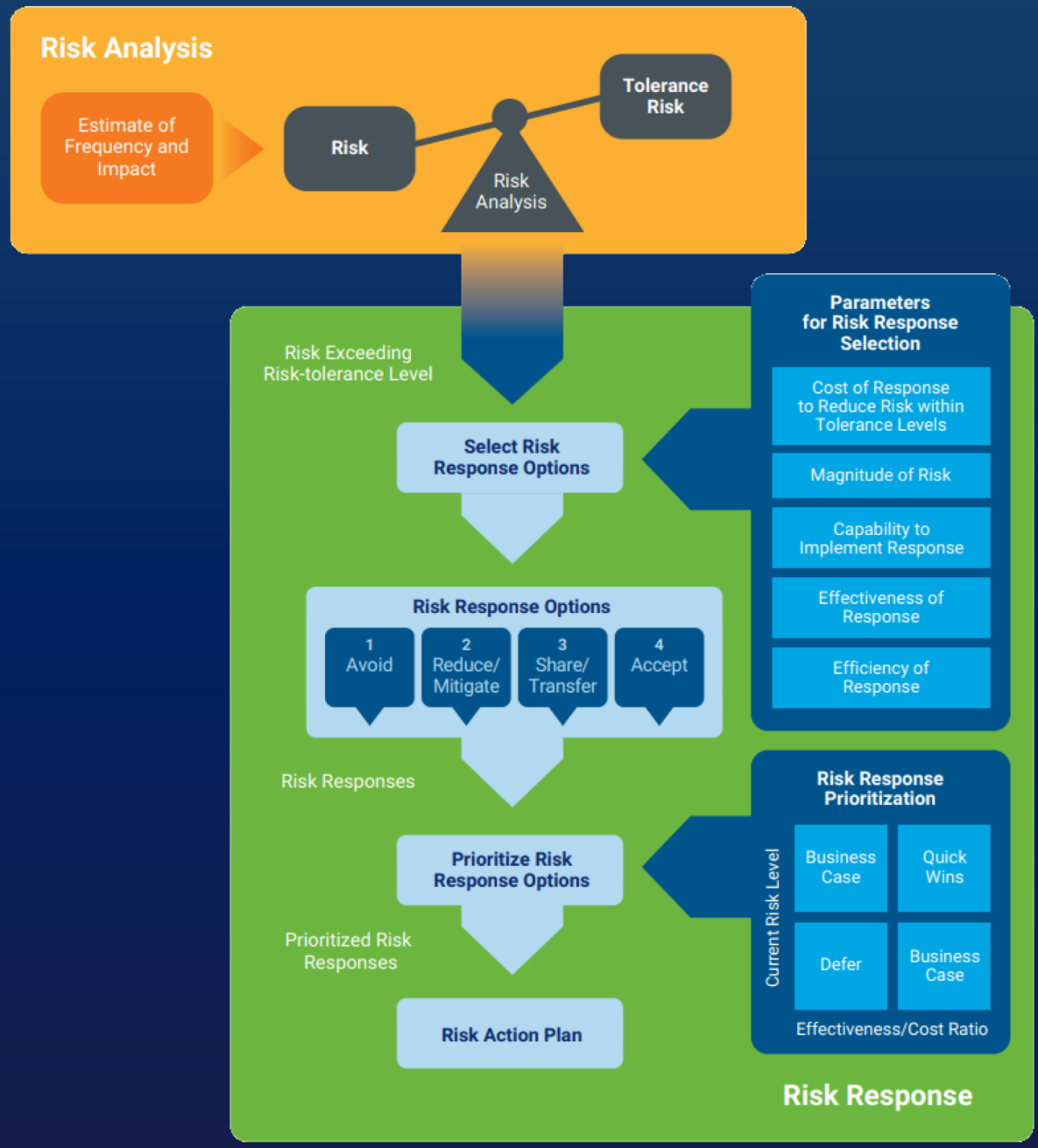
## Risk Management Flow


## Components of I&T Risk Communication




*Source: ISACA IT Risk Framework*

# Risk Response and Prioritization




*Source: ISACA IT Risk Framework*

# STANDARD, FRAMEWORK AND MANUALS RELATED TO IT RISK MANAGEMENT

# RESOURCES RELATED TO IT RISKS


**Risk Starter Kit**

ISACA created the IT Risk Starter Kit to help users develop an IT Risk Program at their organization. Through detailed templates and guides you'll be able to:

- Establish a consistent, disciplined, and integrated approach to risk management.
- Formalize a governance structure for risk oversight which includes the policies, processes, and control systems that support risk-related decision making. And More...


**Risk Scenarios Starter Pack**

This toolkit, free to ISACA members, includes 10 sample risk scenarios that practitioners can use and tailor to their specific context within their enterprises. Risk scenarios facilitate communication in risk management by constructing a narrative that can inspire people to take action.


**Risk Scenarios Toolkit**

The use of risk scenarios can enhance the risk management effort by helping the risk team understand and explain risk to business process owners and other stakeholders.


**Optimizing Risk Response**

Risk is a part of everyday life, from transportation and travel to business and financial decisions. The digital world is no exception. While information and technology have driven innovation and created new opportunities for businesses worldwide, they are not without peril.


**Digital Operational Resilience in the EU Financial Sector: A Risk-Based**

The 2008 financial crisis was one of the most devastating and far-reaching global recessions in modern history. While the reforms that followed strengthened the resilience of the financial sector, they only indirectly addressed information and communications technology (ICT) and did not fully address digital operational resilience.

*Source: https://www.isaca.org/resources/it-risk*

# STANDARD AND FRAMEWORKS


**Risk IT Framework**

The Risk IT Framework fills the gap between generic risk management concepts and detailed IT risk management. It provides an end-to-end, comprehensive view of risks related to the use of IT and a similarly thorough treatment of risk management, from the tone and culture at the top, to operational issues. In summary, the framework will enable enterprises to understand and manage significant IT risk types, building upon the existing risk related components within the current ISACA frameworks.


**Risk IT Practitioner Guide**

The Risk IT Practitioner Guide provides practical guidance for risk professionals. The guide includes a large variety of practical risk management techniques that can be implemented immediately.


**COBIT Focus Area: Information and Technology Risk Using COBIT 2019**

*COBIT Focus Area: Information & Technology Risk* provides guidance related to information and technology (I&T) risk and how to apply COBIT to I&T risk practices. The publication is based on the COBIT core guidance for governance and management objectives, and it enhances the core guidance by highlighting risk-specific practices and activities as well as providing risk-specific metrics.


**NIST Risk Management Framework**

The Risk Management Framework provides a process that integrates security, privacy, and cyber supply chain risk management activities into the system development life cycle. The risk-based approach to control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders, policies, standards, or regulations.


**ISO 31000 Risk Management**

The long-term success of an organization relies on many things, from continually assessing and updating its offering to optimizing its processes. As if this weren't enough of a challenge, they also need to account for the unexpected in managing risk. That's why we've developed ISO 31000 for risk management.

*Source: https://www.isaca.org/resources/it-risk*

# MANUAL AND CERTIFICATIONS


**CRISC Review Manual**

The *CRISC Review Manual 7th Edition* is a comprehensive reference guide designed to help individuals prepare for the CRISC exam and understand IT-related business risk management roles and responsibilities.


**IT Risk Fundamentals Study Guide**

A comprehensive study aid that will help to prepare learners for the IT Risk Fundamentals Certificate exam. The course offers foundational knowledge of IT-related risk management and the methodology that includes risk identification, evaluation, and response.

**(CRISC) Certified in Risk and Information Systems Control®**

ISACA's Certified in Risk and Information Systems Control (CRISC) certification indicates expertise in identifying and managing enterprise IT risk and implementing and maintaining information systems controls. Gain instant recognition and credibility with CRISC and boost your career.

**IT Risk Fundamentals Certificate**

Ideal for professionals who wish to learn about risk and information and technology (I&T)-related risk, whom currently interact with risk professionals, or are new to risk and interested in working as a risk or IT Risk profession. Affirm your foundational knowledge of risk that is related to I&T.

*Source: https://www.isaca.org*

# THANK YOU FOR YOUR ATTENTION