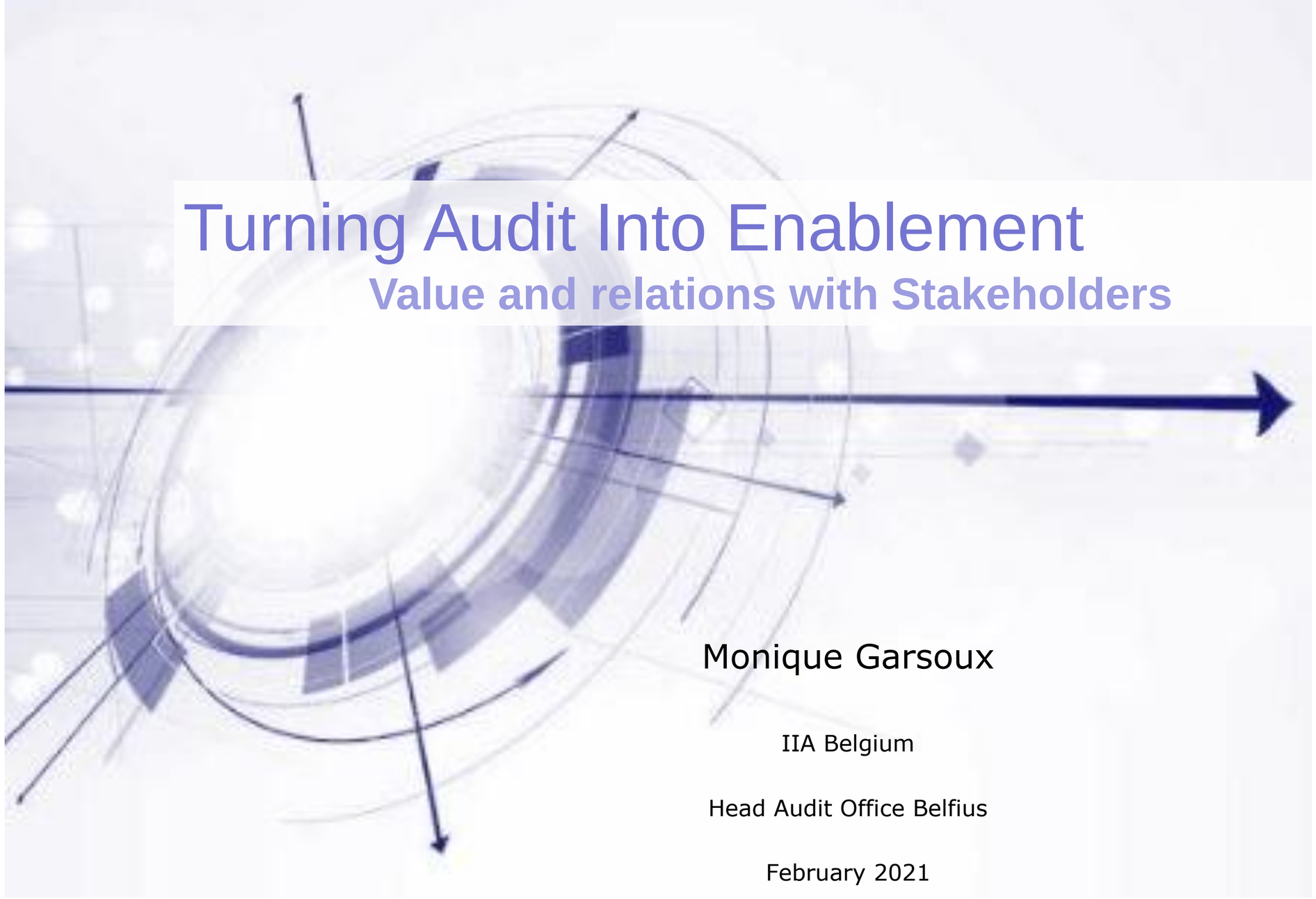
GRC Be Connected

Turning Audit into Enablement

23 February 2021

Programme

Time	Topic	Speaker
1:00 pm -1:05 pm	Welcome	Mrs. Giselle Vercauteren President ISACA Belgium
1:05 pm -1:45 pm	Value and Relations with Stakeholders	Mrs. Monique Garsoux Head of Audit Office Belfius
1:45 pm - 2:15 pm	The benefits you can derive from IT Audit	Professor Georges Ataya Solvay Brussels School of Economics & Management
2:15 pm - 2:55 pm	Anatomy of an Audit assignment	Mrs. Kelly Hogan, Consultant Audit Consulting and Training, LLC
2:55 pm - 3:00 pm	Wrap-up & closure of the meeting	Mrs. Giselle Vercauteren President ISACA Belgium



Turning Audit Into Enablement

Value and relations with Stakeholders

Monique Garsoux

IIA Belgium

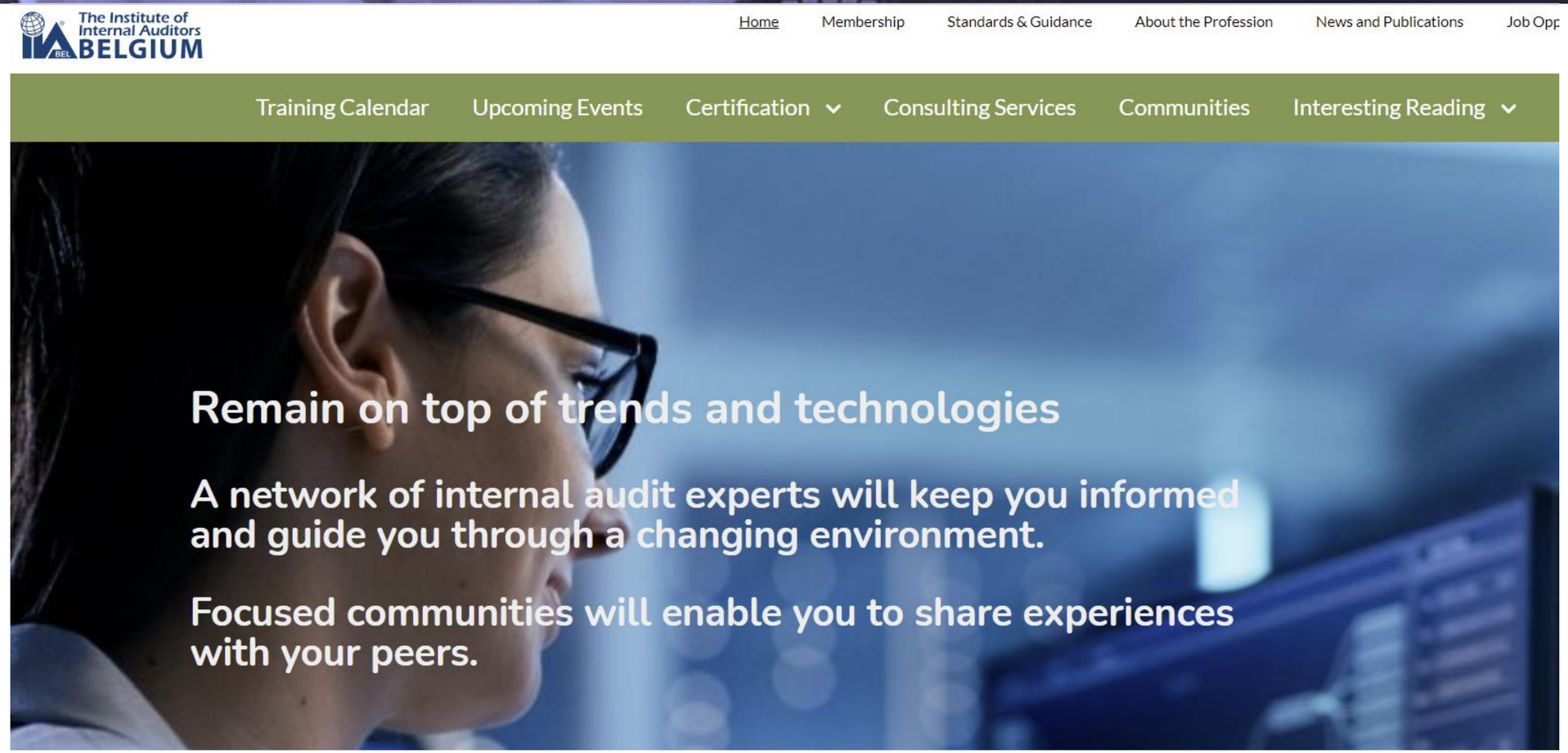
Head Audit Office Belfius

February 2021

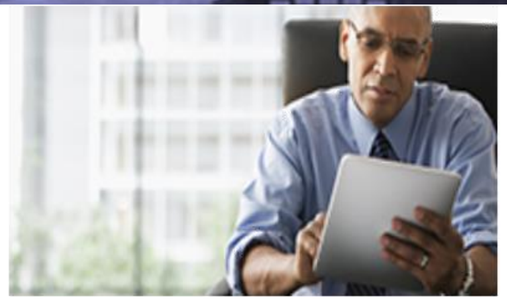
IIA Global Who we are ?

- International Professional Association
- Established in 1941
- Global Headquarters –U.S.A.
- More than 170,000 members worldwide
- Representation in more than 165 countries

IIA Belgium


The Institute of Internal Auditors BELGIUM
Home
Membership
Standards & Guidance
About the Profession
News and Publications
Job Opp
Training Calendar
Upcoming Events
Certification
Consulting Services
Communities
Interesting Reading
Remain on top of trends and technologies
A network of internal audit experts will keep you informed and guide you through a changing environment.
Focused communities will enable you to share experiences with your peers.

What Audit Intends to do



Mission of Internal Audit

The Mission of Internal Audit articulates what internal audit aspires to accomplish within an organization. Its place in the new IPPF is deliberate, demonstrating how practitioners should leverage the entire framework to facilitate their ability to achieve the Mission:

To enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight.

Mandatory Guidance

Mandatory guidance is developed following an established due diligence process, which includes a period of public exposure for stakeholder input. The mandatory elements of the IPPF are:

- Core Principles for the Professional Practice of Internal Auditing
- Definition of Internal Auditing
- Code of Ethics
- *International Standards for the Professional Practice of Internal Auditing*

Recommended Guidance

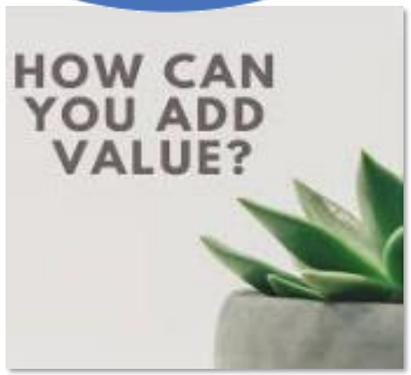
Recommended guidance is endorsed by The IIA through a formal approval process. It describes practices for effective implementation of The IIA's Core Principles, Definition of Internal Auditing, Code of Ethics, and *Standards*. The recommended elements of the IPPF are:

- Implementation Guidance
- Supplemental Guidance

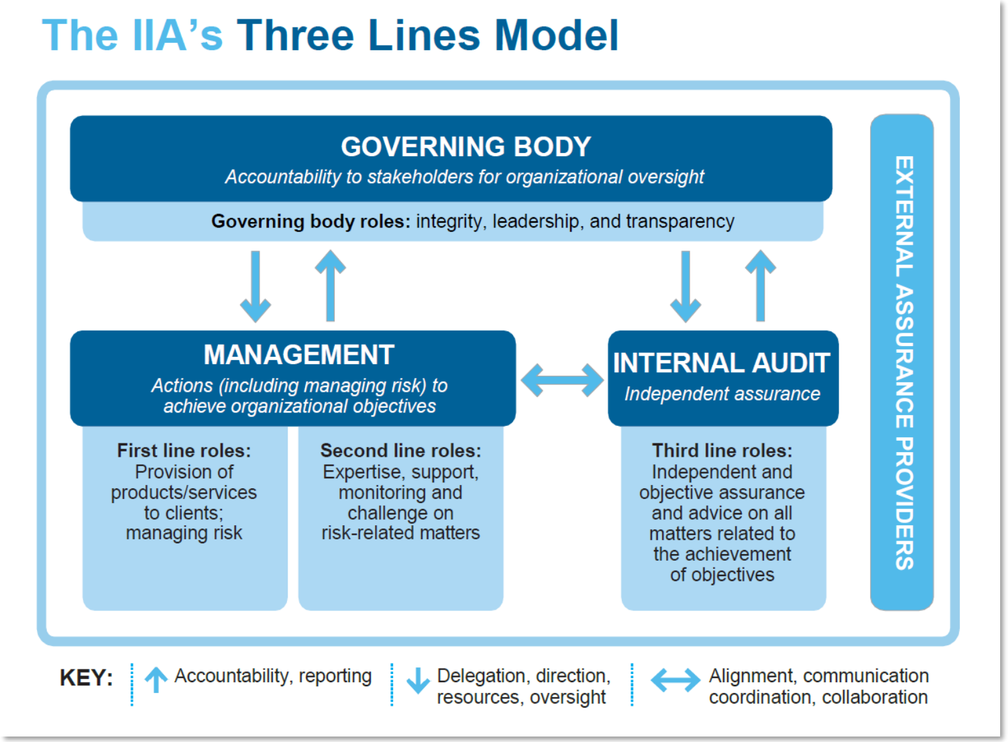
To enhance and protect organizational value by providing risk-based and objective assurance, advice and insight

What Internal Audit Does

"Internal auditing is an independent, objective assurance and consulting activity designed to **add value** and improve an organisation's operations. It helps an organisation accomplish **its objectives** by bringing a **systematic, disciplined approach** to evaluate and improve the effectiveness of **risk management**, **control**, and **governance processes**."



Who are our stakeholders ?



- Audit Customers (Auditees)
- Management Board
- Audit Committee , BOD
- External Audit
- Regulators

Added Value all stakeholders

Trusted partners

Confidence
Transparency
Exchange of information
Agility
Key correspondents
Dialogue on risks

- Workgroups
- Meetings
- Facilitator
- GRC
- Projects

Stakeholders

Roles and Responsibilities
Processes
Objectives
Governance, Risks & Controls

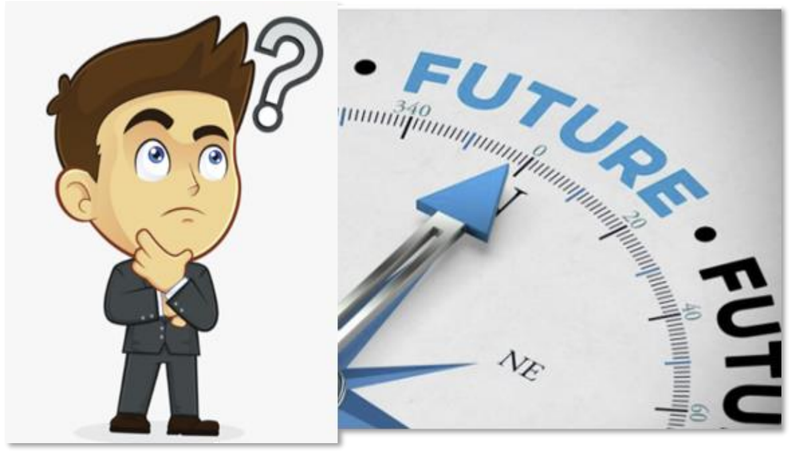
Audit

Risk Assessment

Audit work
Mission and Advice

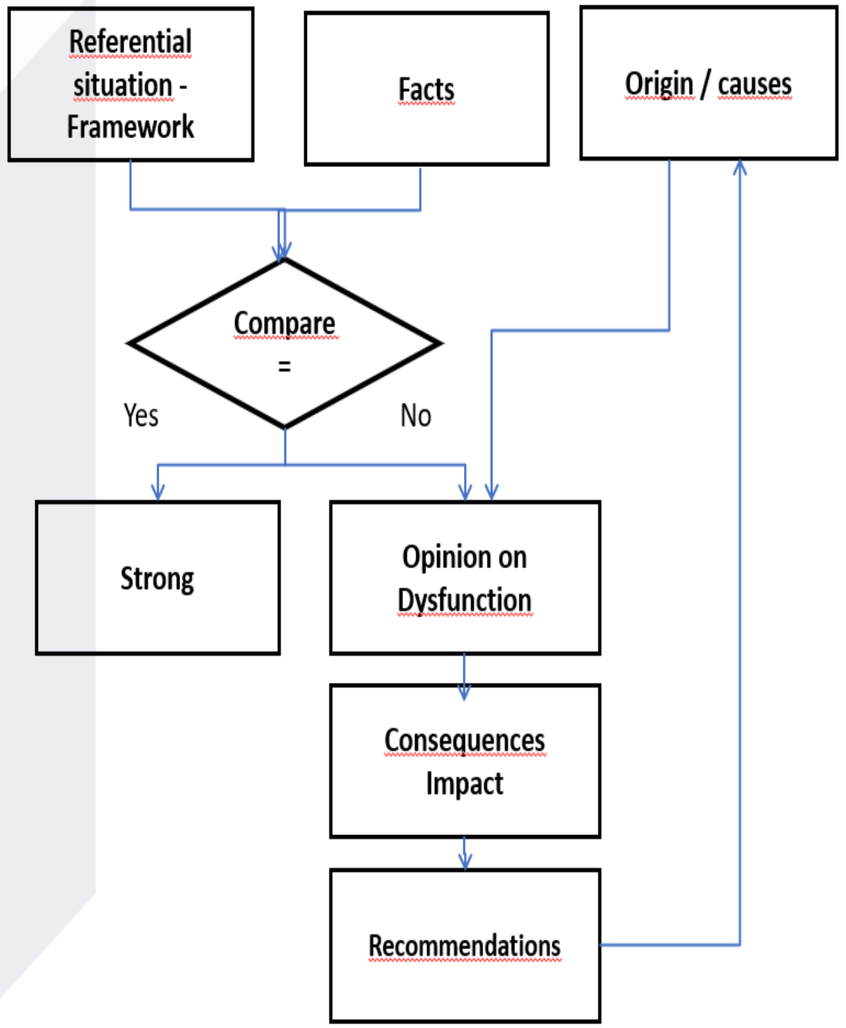
The next step to Enablement ?

- Advisor
- Mutual reliance
- Combined assurance and reporting

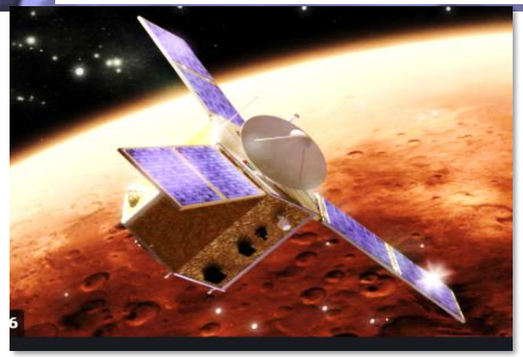


- The Challenge
- Thoughts leader
- New added value :
  - anticipating **emerging** risks and trends

HOW : FRAMEWORKS AND REFERENCES



HOW TURNING AUDIT CLIENTS INTO ALLIES
THE MISSION METHODOLOGY



ANNUAL RISK ASSESSMENT

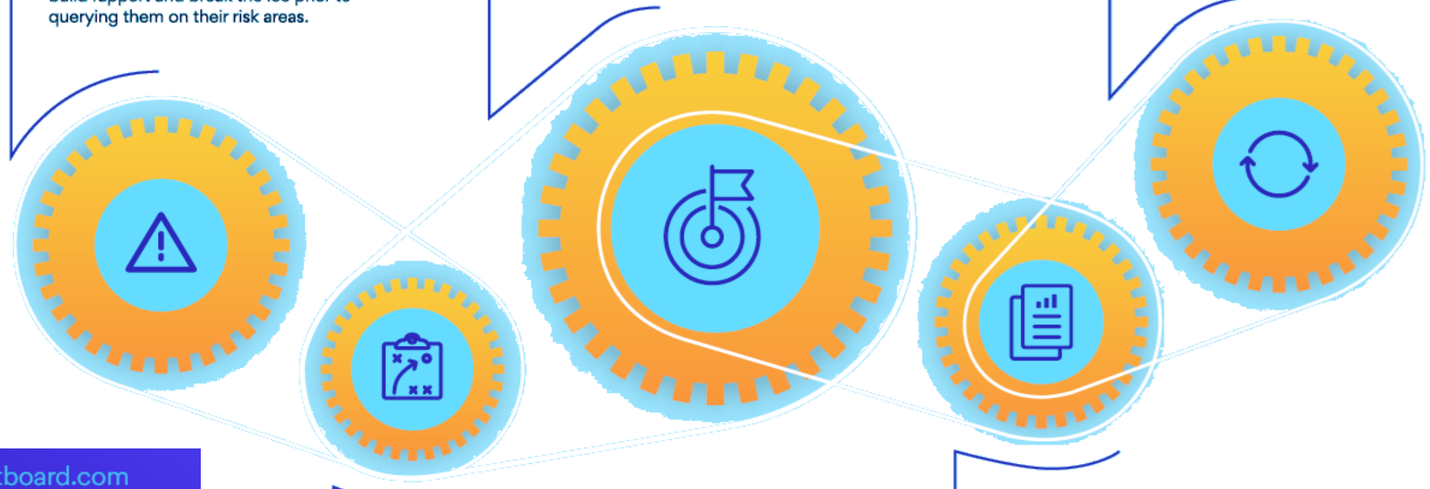
- Meet your key stakeholders face to face to build rapport and break the ice prior to querying them on their risk areas.

FIELDWORK

- Lay out a clear and concise plan for communicating with clients during the opening meeting, include dates of meetings, check-ins, and closing meeting.
- Schedule a weekly meeting with the main point(s) of contact to review the working results as the project unfolds.

OFF-CYCLE/THROUGHOUT THE YEAR

- Get to know your regular audit clients well when you're not in the middle of an audit or requesting help from them. Meet with them to get coffee (or virtual coffee) and learn about their lives. By establishing a genuine interest and investment in the relationship, you'll be building allies rather than adversaries.



auditboard.com

Copyright © 2021 AuditBoard Inc.

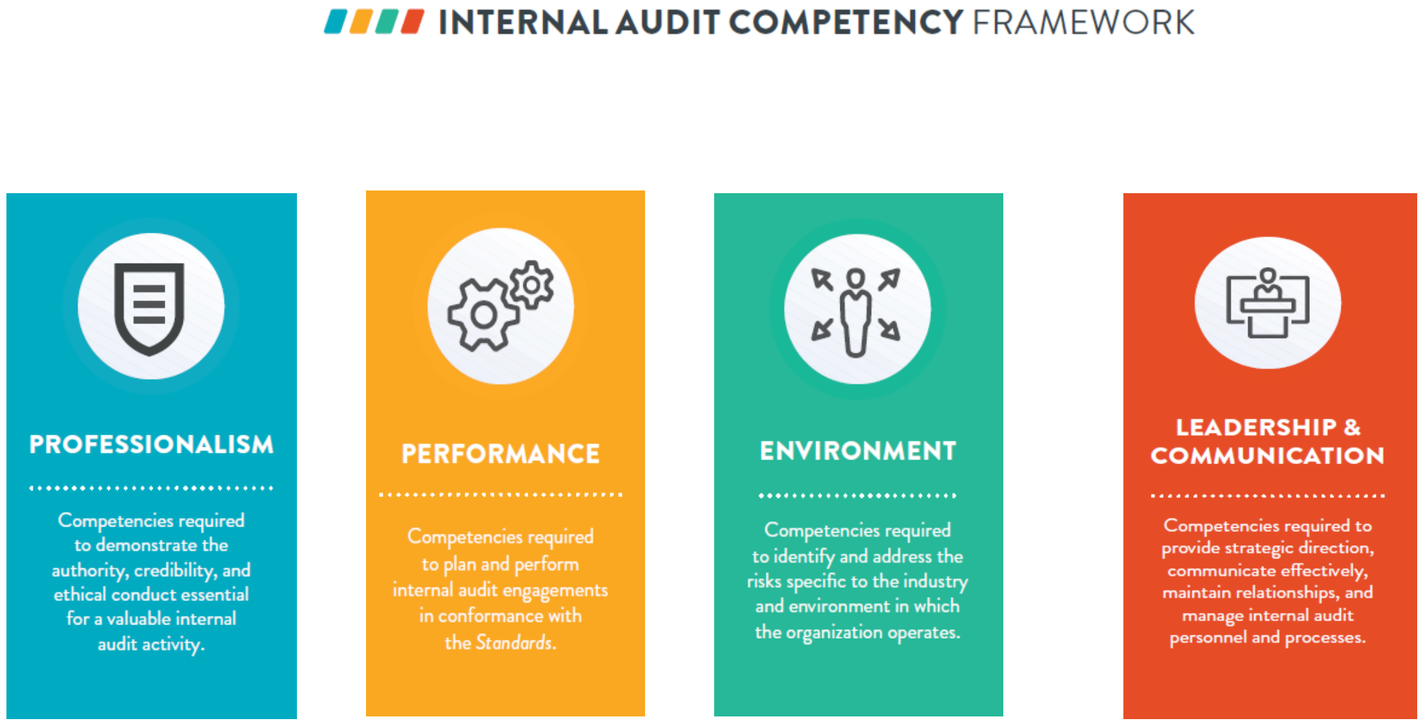
PLANNING

- Communicate with stakeholders/process owners well in advance of the audit (exception: surprise audits).
- Provide clear dates, and stick to them. Don't push back meetings or announce unexpected meetings.
- Be mindful of the client's location and timezone. Run planning calls during the client's working hours.
- Leverage an audit management solution to facilitate communication with clients and streamline document requests.

REPORTING

- Ensure stakeholders and points of contact have been briefed on preliminary audit findings in advance of the closing meeting.
- If cross-functional teams are involved, brief them on the findings prior to the closing meeting.
- Come to the closing meeting prepared with draft management action plans.

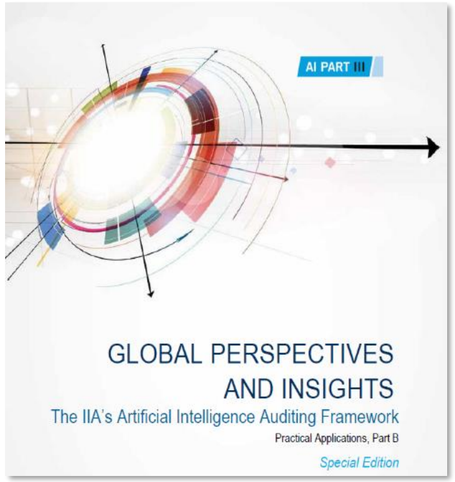
HOW AUDIT COMPETENCY AND KNOWLEDGE

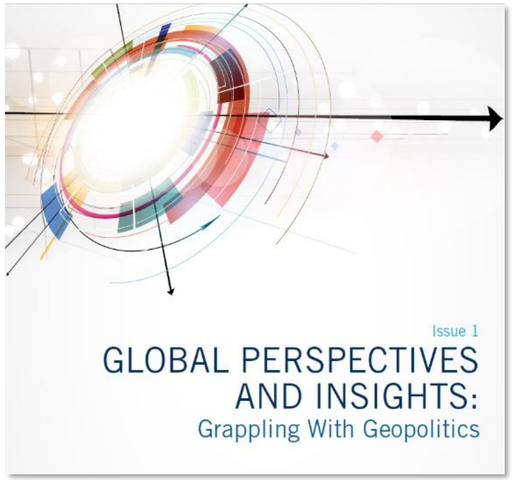


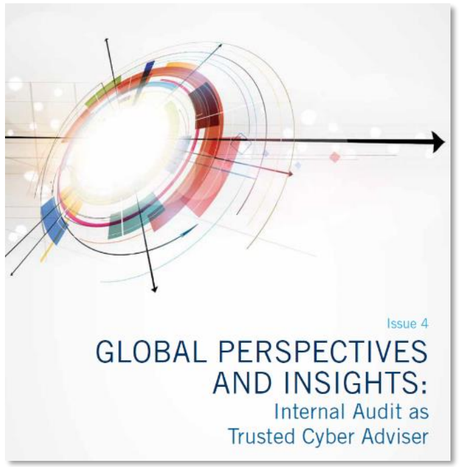
A real need but :

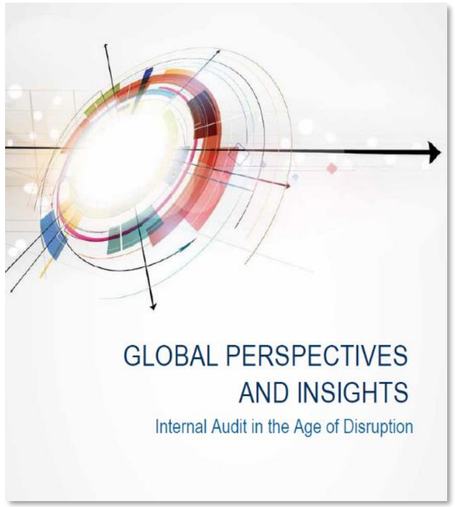
It is not just about **competence** in Internal Audit and **knowledge**

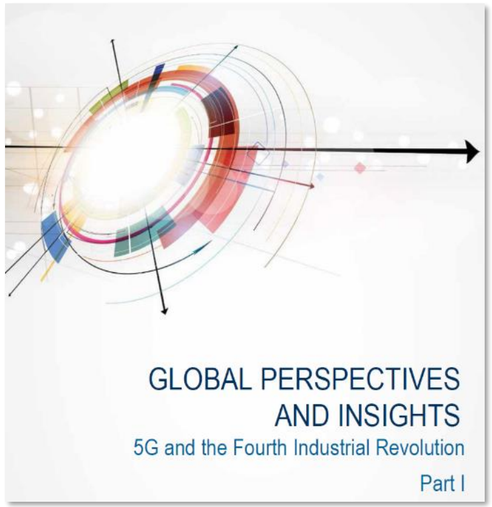
How / a lot of papers







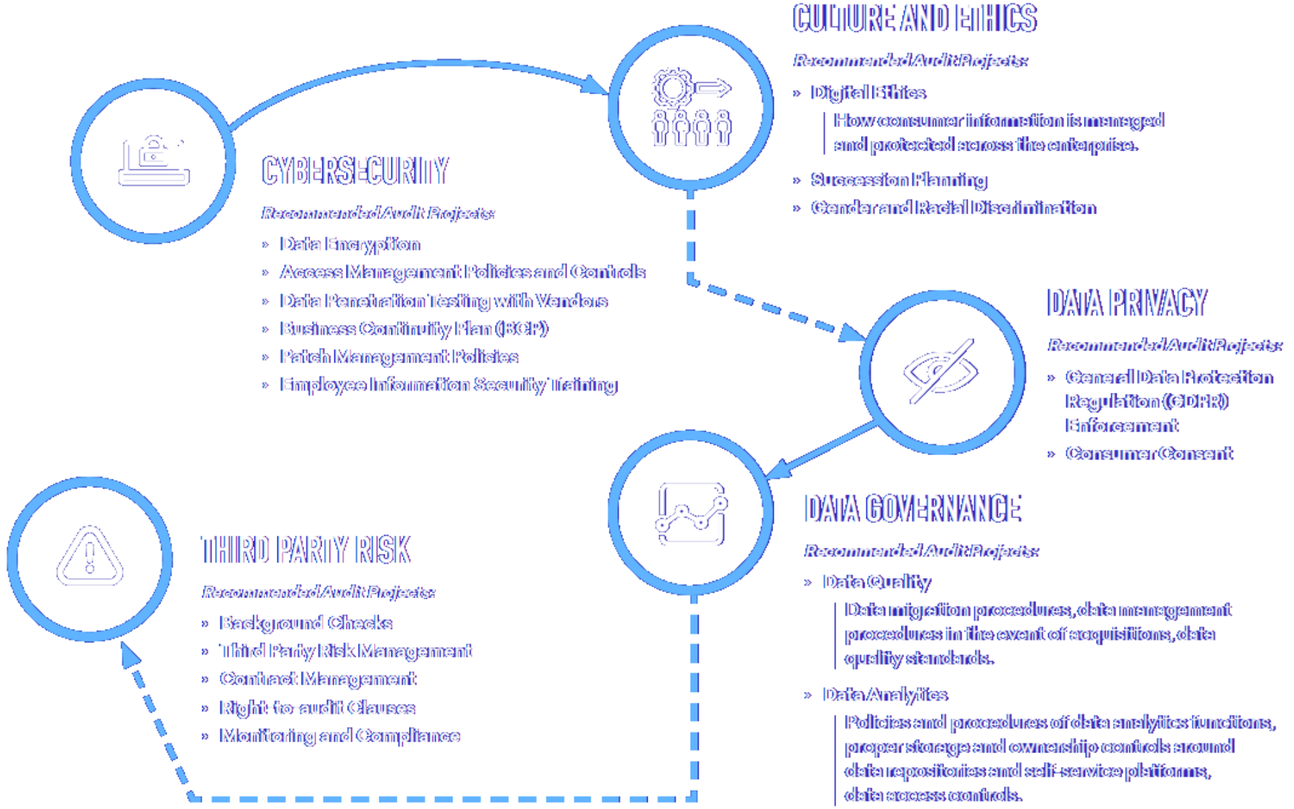




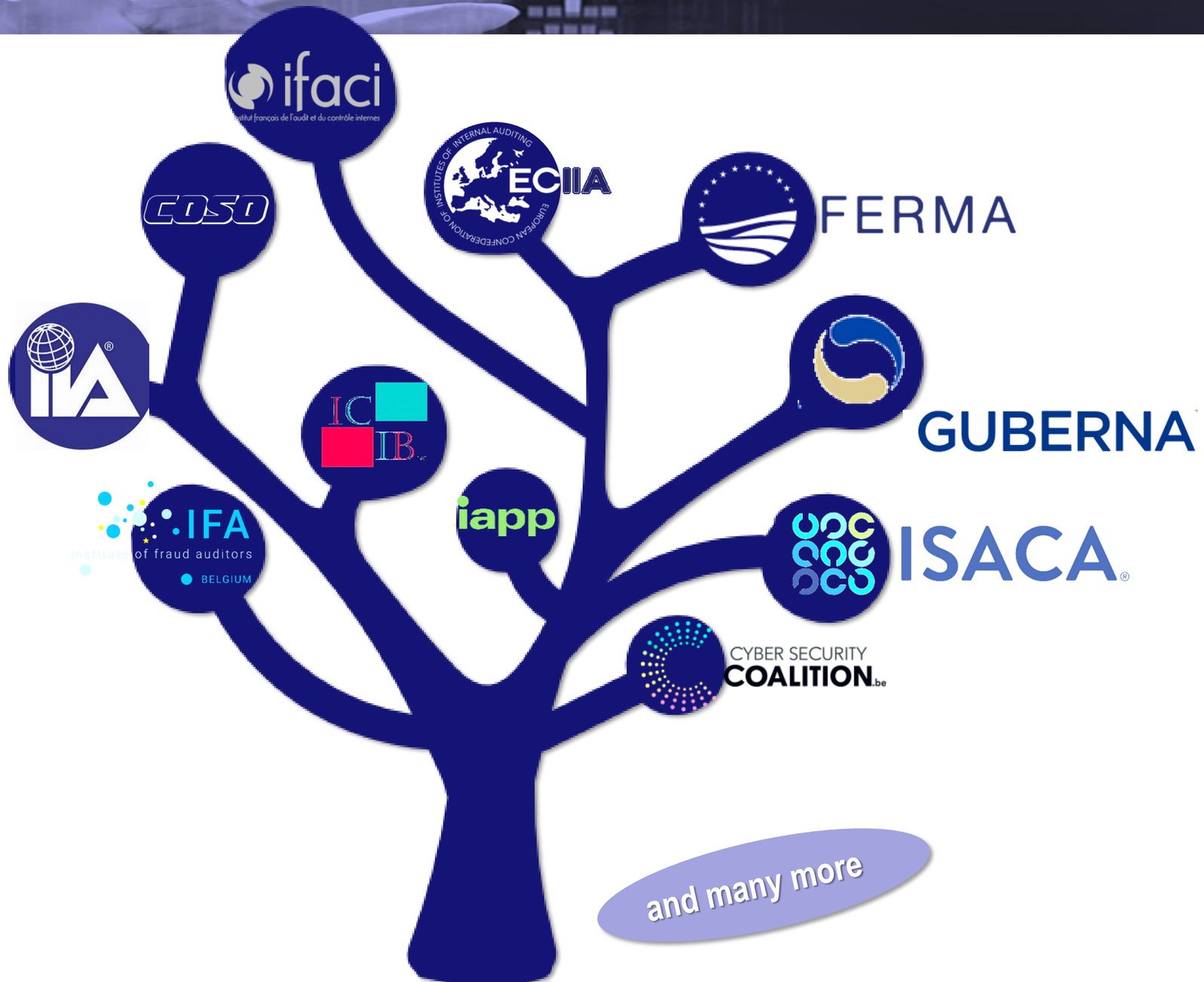
Social media

How / a lot of papers

5 CRITICAL RISK AREAS TO INCLUDE IN YOUR AUDIT PLAN



HOW INTERESTING ASSOCIATIONS



Questions

The benefits you can derive from IT audit

As an auditor, as a client or as an audit-savvy professional

Prof. Georges Ataya, CISA, CISM, CGEIT, CRISC

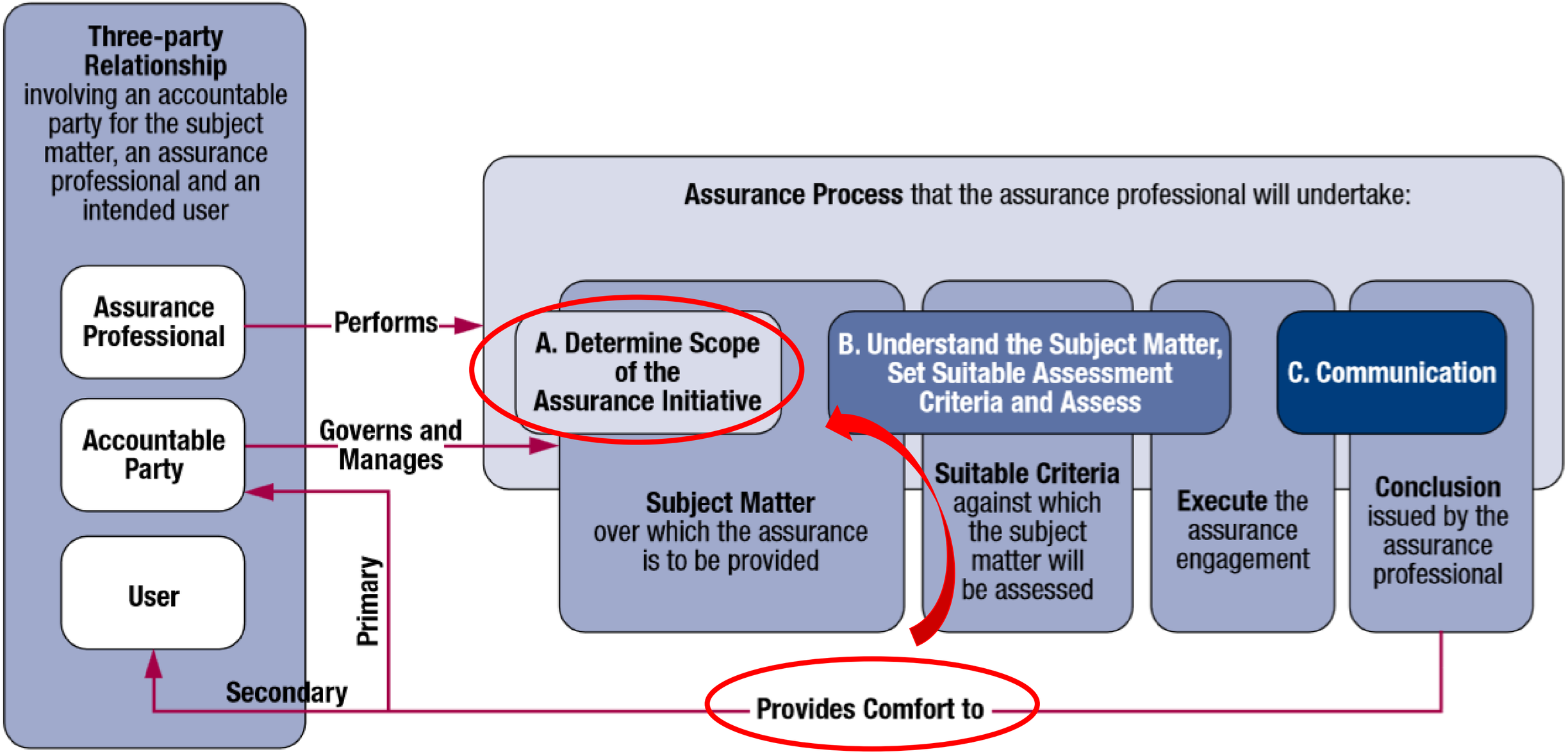
23 February 2021

Georges Ataya

- Past International Senior IT Auditor (ITT Corporation)
- Past Partner EY, General Manager (EY Technology and security Risk Services)
- Past President ISACA Belgium
- Certified Expert witness towards at the Belgium Justice federal service
- Past International Vice President ISACA and the IT Governance institute
- Member of the Belgian Federal Audit Committee (Office of the prime Minister)
- Lecturing Audit since 2001
- Certified IS Auditor Credential (CISA)

Linkedin/be/ataya

AUDIT AS A THREE-PARTY RELATIONSHIP


Three-party Relationship
involving an accountable party for the subject matter, an assurance professional and an intended user
Assurance Professional
Accountable Party
User
Performs
Governs and Manages
Primary
Secondary
Assurance Process that the assurance professional will undertake:
A. Determine Scope of the Assurance Initiative
B. Understand the Subject Matter, Set Suitable Assessment Criteria and Assess
C. Communication
Subject Matter over which the assurance is to be provided
Suitable Criteria against which the subject matter will be assessed
Execute the assurance engagement
Conclusion issued by the assurance professional
Provides Comfort to

Audit Universe vs Assignment Scope

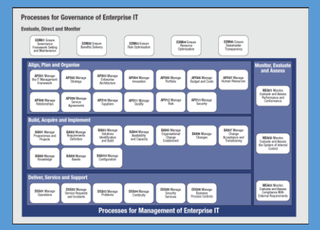
What does management hope to obtain as a result of the assurance initiative?

Audit Universe

Global Risk assessment result

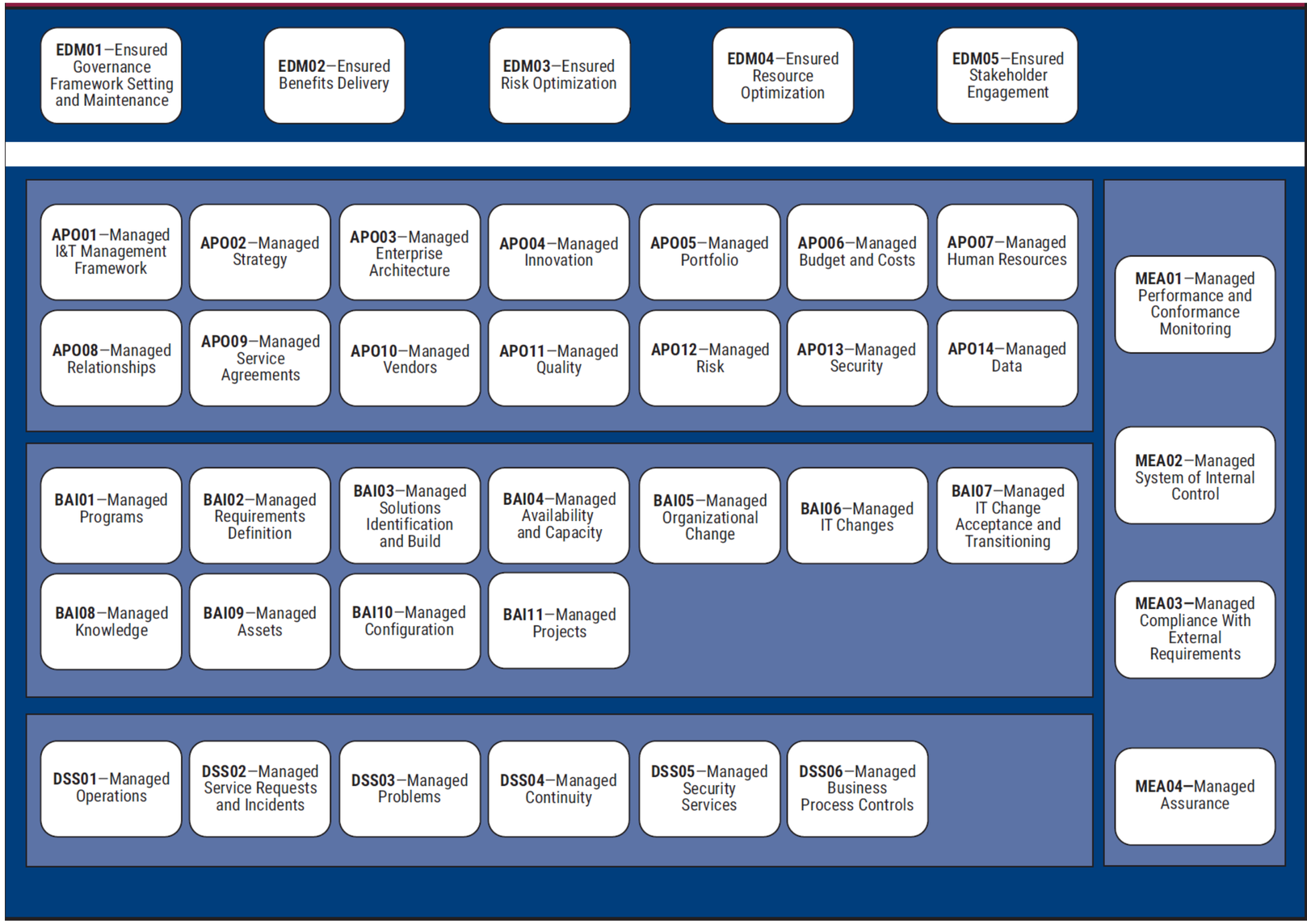
Assessment scope based on comfort statement

Audit assignment scope



Suitable Criteria

Criteria are the standards and benchmarks, such as COBIT 2019, used to measure and present the subject matter and against which the practitioner evaluates the subject matter.



Domain: Build, Acquire and Implement Management Objective: BAI09 — Managed Assets	Focus Area: COBIT Core Model

Description

Manage I&T assets through their life cycle to make sure that their use delivers value at optimal cost, they remain operational (fit for purpose), and they are accounted for and physically protected. Ensure that those assets that are critical to support service capability are reliable and available. Manage software licenses to ensure that the optimal number are acquired, retained and deployed in relation to required business usage, and the software installed is in compliance with license agreements.

Purpose

Account for all I&T assets and optimize the value provided by their use.

B. Component: Organizational Structures

Key Management Practice	Chief Information Officer	Chief Technology Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Privacy Officer
BAI09.01 Identify and record current assets.		A			R	R			
BAI09.02 Manage critical assets.		A	R	R	R	R		R	R
BAI09.03 Manage the asset life cycle.		A			R	R	R		
BAI09.04 Optimize asset value.	A	R	R	R	R	R	R		
BAI09.05 Manage licenses.	A	R		R	R	R			

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

Identify Management Components

BAI09.04 Optimize asset value. Regularly review the overall asset base to identify ways to optimize value in alignment with business needs.	a. Benchmark costs b. Number of assets not utilized
Activities	**Capability Level**
1. On a regular basis, review the overall asset base, considering whether it is aligned with business requirements.	3
2. Assess maintenance costs, consider reasonableness, and identify lower-cost options. Include, where necessary, replacement with new alternatives.	4
3. Review warranties and consider value-for-money and replacement strategies to determine lowest-cost options.	5
4. Use capacity and utilization statistics to identify underutilized or redundant assets that could be considered for disposal or replacement to reduce costs.	
5. Review the overall base to identify opportunities for standardization, single sourcing, and other strategies that may lower procurement, support and maintenance costs.	
6. Review the overall state to identify opportunities to leverage emerging technologies or alternative sourcing strategies to reduce costs or increase value-for-money.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

Processes

E. Component: Policies and Procedures	
Relevant Policy	**Policy Description**
Asset management policy	Provides guidelines for asset life cycle management, asset protection measures, system classification and ownership, data ownership, and data classification
Intellectual property (IP) policy	Addresses risk related to use, ownership, sale and distribution of the outputs of I&T-related creative endeavors by employees (e.g., software development). Mandates appropriate documentation, level of detail, etc., from inception of work.

Principles, policies and frameworks

C. Component: Information Flows and Items (see also Section 3.6)				
Management Practice	**Inputs**		**Outputs**	
	From	**Description**	**Description**	**To**
BAI09.01 Identify and record current assets.	BAI03.04	Updates to asset inventory	Results of fit-for-purpose reviews	APO02.02
	BAI10.02	Configuration repository	Asset register	APO06.01; BAI10.03
			Results of physical inventory checks	BAI10.03; BAI10.04; DSS05.03
BAI09.02 Manage critical assets.			Communications of planned maintenance downtime	APO08.04
			Maintenance agreements	Internal
BAI09.03 Manage the asset life cycle.			Authorized asset retirements	BAI10.03
			Updated asset register	BAI10.03
			Approved asset procurement requests	Internal

Information

G. Component: Services, Infrastructure and Applications
Asset management tools

Services, infrastructure and applications

Audit opportunities

Auditor

- Act as an auditor not as a consultant
- Focus on the client's request
- Justify every conclusion

Audit-savvy professional

- Auditee's opportunity to report issues upwards
- Use findings to prove your resources needs and risks posture

Audit client

- Opportunity to use auditor expertise as a second opinion
- Auditors could be the best allies

Certified Information Systems Auditor®

An ISACA® Certification

151K+
CISA CERTIFICATION HOLDERS

US $110K+
AVERAGE SALARY OF CISA HOLDERS

ANSI Accredited Program Personnel Certification
CISA ACCREDITED UNDER
ISO/IEC 17024:2012

THE CISA DIFFERENCE

Whether you are seeking a new career opportunity or striving to grow within your current organization, a CISA certification proves your expertise in these work-related domains:

- INFORMATION SYSTEMS AUDITING PROCESS
- GOVERNANCE AND MANAGEMENT OF IT
- INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND IMPLEMENTATION
- INFORMATION SYSTEMS OPERATIONS AND BUSINESS RESILIENCE
- PROTECTION OF INFORMATION ASSETS

Domain 1—INFORMATION SYSTEMS AUDITING PROCESS - (21%)

Providing audit services in accordance with standards to assist organizations in protecting and controlling information systems. Domain 1 affirms your credibility to offer conclusions on the state of an organization’s IS/IT security, risk and control solutions.

A. Planning

1. IS Audit Standards, Guidelines, and Codes of Ethics
2. Business Processes
3. Types of Controls
4. Risk-Based Audit Planning
5. Types of Audits and Assessments

B. Execution

1. Audit Project Management
2. Sampling Methodology
3. Audit Evidence Collection Techniques
4. Data Analytics
5. Reporting and Communication Techniques

Domain 2—Governance and Management of IT - (17%)

Domain 2 confirms to stakeholders your abilities to identify critical issues and recommend enterprise-specific practices to support and safeguard the governance of information and related technologies.

A. IT Governance

IT Governance and IT Strategy

IT-Related Frameworks

IT Standards, Policies, and Procedures

Organizational Structure

Enterprise Architecture

Enterprise Risk Management

Maturity Models

Laws, Regulations, and Industry Standards affecting the Organization

B. IT Management

IT Resource Management

IT Service Provider Acquisition and Management

IT Performance Monitoring and Reporting

Quality Assurance and Quality Management of IT

Domain 3—Information Systems Acquisition, Development and Implementation - (12%)

A. Information Systems Acquisition and Development

Project Governance and Management

Business Case and Feasibility Analysis

System Development Methodologies

Control Identification and Design

B. Information Systems Implementation

Testing Methodologies

Configuration and Release Management

System Migration, Infrastructure Deployment, and Data Conversion

Post-implementation Review

Domain 4—INFORMATION SYSTEMS OPERATIONS AND BUSINESS RESILIENCE - (23%)

Domains 3 and 4 offer proof not only of your competency in IT controls, but also your understanding of how IT relates to business.

- **A. Information Systems Operations**

1. Common Technology Components
2. IT Asset Management
3. Job Scheduling and Production Process Automation
4. System Interfaces
5. End-User Computing
6. Data Governance
7. Systems Performance Management
8. Problem and Incident Management
9. Change, Configuration, Release, and Patch Management
10. IT Service Level Management
11. Database Management

- **B. Business Resilience**

1. Business Impact Analysis (BIA)
2. System Resiliency
3. Data Backup, Storage, and Restoration
4. Business Continuity Plan (BCP)
5. Disaster Recovery Plans (DRP)

Domain 5—Protection of Information Assets - (27%)

Cybersecurity now touches virtually every information systems role, and understanding its principles, best practices and pitfalls is a major focus within Domain 5.

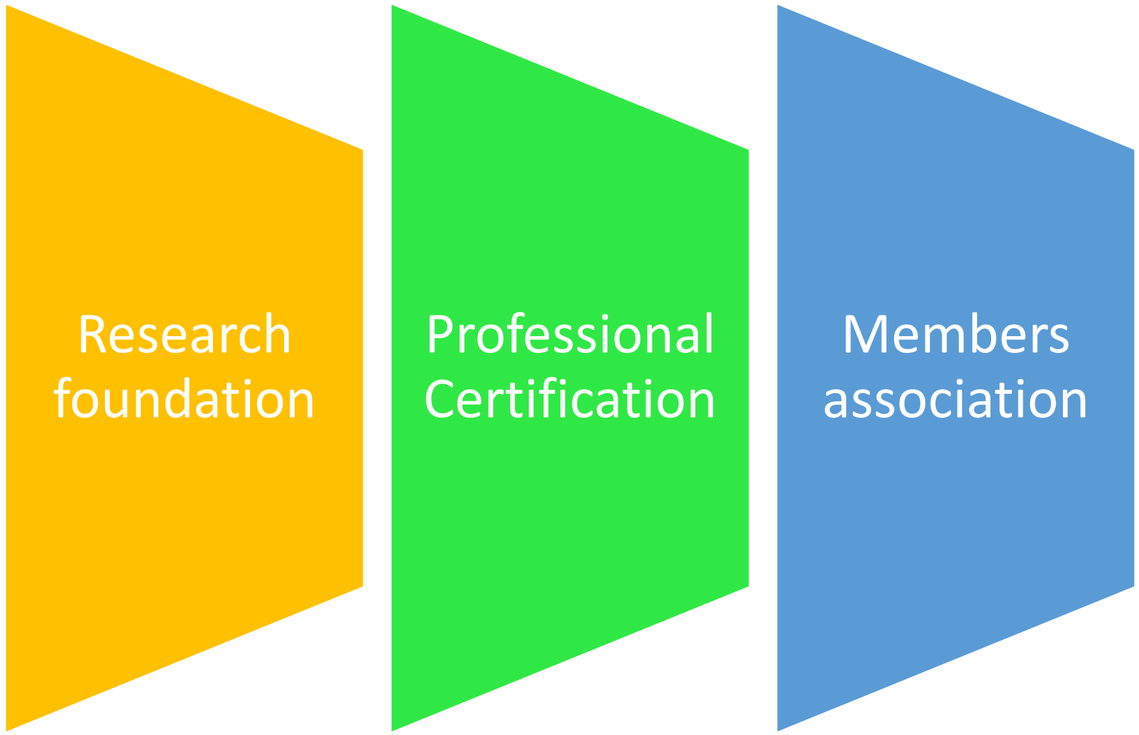
A. Information Asset Security and Control

Information Asset Security Frameworks, Standards, and Guidelines
Privacy Principles
Physical Access and Environmental Controls
Identity and Access Management
Network and End-Point Security
Data Classification
Data Encryption and Encryption-Related Techniques
Public Key Infrastructure (PKI)
Web-Based Communication Techniques
Virtualized Environments
Mobile, Wireless, and Internet-of-Things (IoT) Devices

B. Security Event Management

Security Awareness Training and Programs
Information System Attack Methods and Techniques
Security Testing Tools and Techniques
Security Monitoring Tools and Techniques
Incident Response Management
Evidence Collection and Forensics

ISACA



- Since 1967
- Started as the EDP Auditors association
- Active in 180 countries (Belgium since 1985)
- Later called “Information Systems Audit and Control Association” (not used any more)
- Created the IT Governance Institute in 1999
- Strategic decision to focus on IT governance, Information risk and Information Security in 2008
- ISACA now goes only by its acronym to reflect the broad range of IT governance professionals it serves

ISACA®

165,000+ members worldwide

Search our 200+ chapters worldwide to find one near you.

Learn the benefits of joining a chapter, including the opportunity you'll have to share a broad range of professional expertise from diverse business communities.

https://www.isaca.org/membership/

Invited by G. Ataya member Id 039462

ISACA

COBIT >

Explore the globally recognized framework for the governance of enterprise IT.

INSIGHTS AND EXPERTISE >

Gain insights and grow your know-how with expert-developed white papers, discussions, programs and tools.

FRAMEWORKS, STANDARDS AND MODELS >

Use the right frameworks to add value to your role and enterprise.

ISACA JOURNAL >

Read through peer-reviewed, in-depth articles on pressing industry topics.

NEWS & TRENDS >

Blogs, Podcast and Newsletters. Explore the latest on industry standards, best practices and emerging trends.

Book

CISM Review Questions, Answers & Explanations Manual, 9th Edition

CISM Review Questions, Answers & Explanations Manual 9th Edition consists of 1,000 multiple-choice study questions, answers and...

FREE MEMBER PREVIEW

Book

Security, Audit and Control Features Oracle Database, 3rd Edition

Protecting information assets is challenging for every enterprise, regardless of size and industry™ and it has become an even more...

Book

IT Control Objectives for BASEL II: The Importance of Governance and Risk...

ISACA members can complimentary download in addition to being available to ISACA members as a Complimentary...

FREE to ISACA Members
Not a Member? Join Now

Book

Security Considerations for Cloud Computing

Another publication in the Cloud Computing Vision Series, Security Considerations for Cloud Computing presents practical...

FREE to ISACA Members
Not a Member? Join Now

Book

CISA Review Manual, 27th Edition

CISA Review Manual, 27th Edition is a comprehensive reference guide designed to help individuals prepare for the CISA...

FREE MEMBER PREVIEW

Book

CISA Review Questions, Answers & Explanations Manual, 12th Edition

CISA Review Questions, Answers & Explanations Manual, 12th Edition consists of 1,000 multiple-choice study questions and has been...

FREE MEMBER PREVIEW

Book

CRISC Review Manual, 6th Edition

CRISC Review Manual 6th Edition is a comprehensive reference guide designed to help individuals prepare for the CRISC exam and...

FREE MEMBER PREVIEW

Book

CDPSE Review Manual eBook

The CDPSE Review Manual is a comprehensive reference guide designed to help individuals prepare for the CDPSE exam and...

Book

CDPSE Review Manual eBook

The CDPSE Review Manual is a comprehensive reference guide designed to help individuals prepare for the CDPSE exam and...

Book

ITAF™ Companion Performance Guidelines 2208

ISACA created the Information Technology Audit Sampling guidelines (Guideline 2208) as a companion to its Information...

Book

ITAF, 4th Edition

Get the guidance and techniques that will lend consistency and effectiveness to your audits. The new 4th edition of ITAF outlines...

Book

IT Risk Fundamentals Study Guide

The IT Risk Fundamentals Study Guide is a comprehensive study aid that will help to prepare learners for the IT Risk...

Book

COBIT Focus Area: Information Security

COBIT Focus Area: Information Security provides guidance related to information security and how to apply COBIT to specific...

Book

Risk IT Framework, 2nd Edition

The Risk IT Framework is designed to assist in developing, implementing or enhancing the practice of risk management by...

18 June 2020

Book

Risk IT Practitioner Guide, 2nd Edition

The Risk IT Practitioner Guide is designed to assist in developing, implementing or enhancing the practice of risk management by...

05 June 2020

Book

CGEIT Review Manual, 8th Edition eBook

The CGEIT Review Manual 8th Edition is designed to help individuals prepare for the CGEIT exam and understand the...

Book

COBIT 5: Enabling Processes

A detailed reference guide to the processes defined in the COBIT 5 process reference model. This includes the COBIT 5 goals...

Book

Securing Mobile Devices

Securing Mobile Devices should be read in the context of the existing publications COBIT 5 for Information Security, Business...

Book

Getting Started With GEIT

How do organizations know they are effectively utilizing enterprise technology resources to best realize business goals? Do...

FREE to ISACA Members
Not a Member? Join Now

Book

COBIT 5 for Information Security

Bring Order to Complex Standards and Frameworks:COBIT 5 for Information Security leverages the COBIT 5 framework—the globally...

Book

COBIT 5 for Risk

Effectively managing IT risk helps drive better business performance by linking information and technology risk to the achievema...

FREE MEMBER PREVIEW

Book

COBIT 5 CMMI Practices Pathway Tool

When using framework and standards guidance, you are often faced with making meaningful use of multiple guidance products th...

Book

COBIT 5 DMM Pract Path Tool

The new COBIT® 5/DMM Practices Pathway Tool presents a unique approach to using two specific products, COBIT 5...

Book

COBIT Assessor Guide: Using COBIT 5 & Toolkit

This companion to the COBIT® Process Assessment Model (PAM): Using COBIT® 5 provides details on how to undertake an...

Book

COBIT 5

COBIT 5 framework provides an end-to-end business view of the governance of enterprise IT that reflects the central role of...

FREE MEMBER PREVIEW

Book

COBIT 2019 Framework: Governance and Management Objectives

COBIT is a framework for the governance and management of enterprise information and technology, aimed at the whole...

FREE MEMBER PREVIEW

Book

COBIT 2019 Design Guide: Designing an Information and Technology Governanc...

For more than two decades, the COBIT governance framework for enterprise information and technology (I&T) has been helpin...

FREE MEMBER PREVIEW

Book

COBIT 2019 Framework: Introduction and Methodology

Over the years, best-practice frameworks have been developed and promoted to assist in the process of understanding...

FREE MEMBER PREVIEW

Book

COBIT 2019 Implementation Guide: Implementing and Optimizing an Information...

In this age of digital transformation, enterprises are more dependent than ever on information and technology (I&T)...

FREE MEMBER PREVIEW

Book

COBIT 2019 Design Guide and Toolkit: Designing an Information & Technology...

For more than two decades, the COBIT governance framework for enterprise information and technology (I&T) has been helpin...

FREE to ISACA Members
Not a Member? Join Now

Book

COBIT 4_1

COBIT 4.1 refines and fine-tunes the material presented in COBIT 4.0—the first major update of the COBIT core content since the...

Book

CISM Review Manual, 15th Edition

CISM Review Manual 15th Edition is designed to help you prepare for the CISM exam. This comprehensive, easy-to-navigate...

FREE MEMBER PREVIEW

Book

Blockchain Framework and Guidance

Blockchain and distributed ledger technologies are poised to take on applications across the breadth of the global digital economy. Trust ...

Book

Blockchain - An Executive View

Blockchain and distributed ledger technologies are poised to take on applications across the breadth of the global digital economy. Trust ...

Book

A Practical Guide to the Payment Card Industry Data Security Standard (PCI DSS)

This book explains the security requirements, processes and technologies that are required to implement the Payment Card...

Book

Blockchain Fundamentals

Blockchain has the potential to become a major force for innovation and change the way you process everything with...

Book

Creating a Culture of Security

No security policies, standards, guidelines or procedures can foresee all of the circumstances in which they are to be interpreted...

FREE to ISACA Members
Not a Member? Join Now

Book

IT Governance and Process Maturity

In addition to being available to ISACA members as a Complimentary download,nonmembers of ISACA...

FREE to ISACA Members
Not a Member? Join Now

Book

Information Security Governance: Guidance for Information Security...

In addition to being available to ISACA members as a Complimentary download, nonmembers of ISACA can...

FREE to ISACA Members
Not a Member? Join Now

Book

Responding to Targeted Cyberattacks

A Breach WILL Eventually Occur! Is your enterprise prepared? The threat environment has radically changed over the last decade...

Book

Implementing Cybersecurity Guidance for Small and Medium-sized Enterprises

Cybersecurity is a topic of interest for most enterprises, regardless of their size. Cybercrime and cyberwarfare are not restricted to...

Book

Transforming Cybersecurity

The cost and frequency of cybersecurity incidents are on the rise. Is your enterprise keeping pace? The numbers of threats, ris...

Book

Implementing the NIST Cybersecurity Framework

In 2013, US President Obama issued Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, which...

Book

Cybersecurity Guidance for Small and Medium-Sized Enterprises

Cybersecurity is rapidly becoming a critical activity in many enterprises, due to the increasing number of cyberattacks and...

Book

Advanced Persistent Threats: How to Manage the Risk to Your Business

This book explains the nature of the security phenomenon known as the advanced persistent threat (APT). It also provides helpful...

Book

Guide to China's Regulatory Cybersecurity Implementation Framework

China solicited public comment on the Cybersecurity Law of the People's Republic of China (National Cybersecurity Law)...

Book

CSX Cybersecurity Fundamentals Study Guide, 2nd Edition

The Cybersecurity Fundamentals Study Guide is a comprehensive study aid that will help to prepare learners for the Cybersecurity...

Book

CRISC Review Questions, Answers & Explanations Manual, 5th Edition

CRISC Review Questions, Answers & Explanations Manual, 5th Edition has been expanded and updated to include even more practice...

FREE MEMBER PREVIEW

ISACA Journal

Volume 2, 2020

ISACA Journal

Volume 1, 2020

2018

ISACA Journal

Volume 6, 2018

ISACA Journal

Volume 5, 2018

ISACA Journal

Volume 4, 2018

ISACA Journal

Volume 3, 2018

ISACA Journal

Volume 6, 2019

2019

ISACA Journal

Volume 5, 2019

ISACA Journal

Volume 4, 2019

ISACA Journal

Volume 3, 2019

ISACA Journal

Volume 2, 2018

ISACA Journal

Volume 1, 2018

ISACA Journal

Volume 2, 2019

ISACA Journal

Volume 1, 2019

2017

ISACA Journal

Volume 6, 2017

ISACA Journal

Volume 5, 2017

ISACA Journal

Volume 4, 2017

ISACA Journal

Volume 3, 2017

It's All Right Here!

All of ISACA's timely and industry-leading articles, blogs and podcasts, in one place.

Domain

- [ ] Audit & Assurance
- [ ] Governance
- [ ] Information Security
- [ ] Privacy
- [ ] Risk

Product Type

- [ ] Article
- [ ] Blog
- [ ] Podcast

Article Type

- [ ] @ISACA
- [ ] Blog

Results 1-12 of 2,886

RELEVANCY DATE

BLOG POST

Creatively Scaling Application Security Coverage and Depth

One of the biggest challenges and opportunities for an Application Security (AppSec) team is to scale effectively.

18 February 2021

BLOG POST

Baselining Cybersecurity Skills for All IT Professionals

In the era of modern IT, it is becoming increasingly important for IT professionals to have a base-line contemporary cybersecurity skillset.

17 February 2021

BLOG POST

Rethinking Information Security Awareness Strategies

In 2000, it was predicted that semantic attacks that target humans and use the vulnerability in information processing capabilities of humans would be the primary attack vector of cybercriminals.

17 February 2021

ISACA JOURNAL ARTICLE

Book Review: Corporate Governance—A Pragmatic Guide for Auditors, Directors, Investors, and Accountants

Vasant Raval's Corporate Governance: A Pragmatic Guide for Auditors, Directors, Investors, and

ISACA

CERTIFICATIONS

CISA
CRISC
CISM
CGEIT
CSX-P
CDPSE
ITCA

The Modular, Stackable, New Credential from ISACA is Coming

CERTIFICATES

COBIT
CSX
CYBER SECURITY AUDIT
IT RISK FUNDAMENTALS
CCAK

ISACA | ENGAGE

Home | Communities | Directory | Events | Browse | Volunteer | Get Started | CommunITy Day

All Communities

Governance

This is a forum to collaborate on all topics related to (IT) Governance. We invite you to participate and share your experience and questions regarding the leadership and organizational structures needed to ensure that IT sustains and extends the organization's strategies and objectives thus enabling an organization to achieve its goals.

Discussions 809 | Libraries 26 | Members 6.3K

member | last person joined 13 hours ago

Information and Cybersecurity

For security leaders and practitioners, time is critical and we cannot always wait for the next major conference to discuss security and cybersecurity issues, best practices, new solutions and more. Setting or keeping organizations on the proper path is critical, and this is the forum to share and validate ideas and best practices.

Discussions 3.7K | Libraries 98 | Members 12.6K

member | last person joined 5 hours ago

Privacy

Join

This is a forum for those professionals who interact with privacy issues to collaborate, share experience, ask questions, and exchange relevant resources. The focus of the discussions should be related to privacy concerns, solutions, awareness training, implementation, compliance, and technology innovations related to privacy.

Discussions 674 | Libraries 22 | Members 1.2K

last person joined 13 hours ago

Rising Professionals

Join

Rising professionals – whether completing their schooling or building momentum in the early stages of their careers – discuss successful approaches for navigating the early stages of their career and accelerating their career growth. Join this group to share guidance and network with other rising professionals who are looking to make their mark in the technology workforce.

Discussions 426 | Libraries 3 | Members 874

last person joined 21 hours ago

RisingProfessionals | Students

Risk Management

This forum is the home of all topics about risk assessment and risk management, including vulnerabilities, threats and risk treatments, methodologies, best practices and tips from practitioners worldwide.

Discussions 1.4K | Libraries 37 | Members 6.7K

member | last person joined 13 hours ago

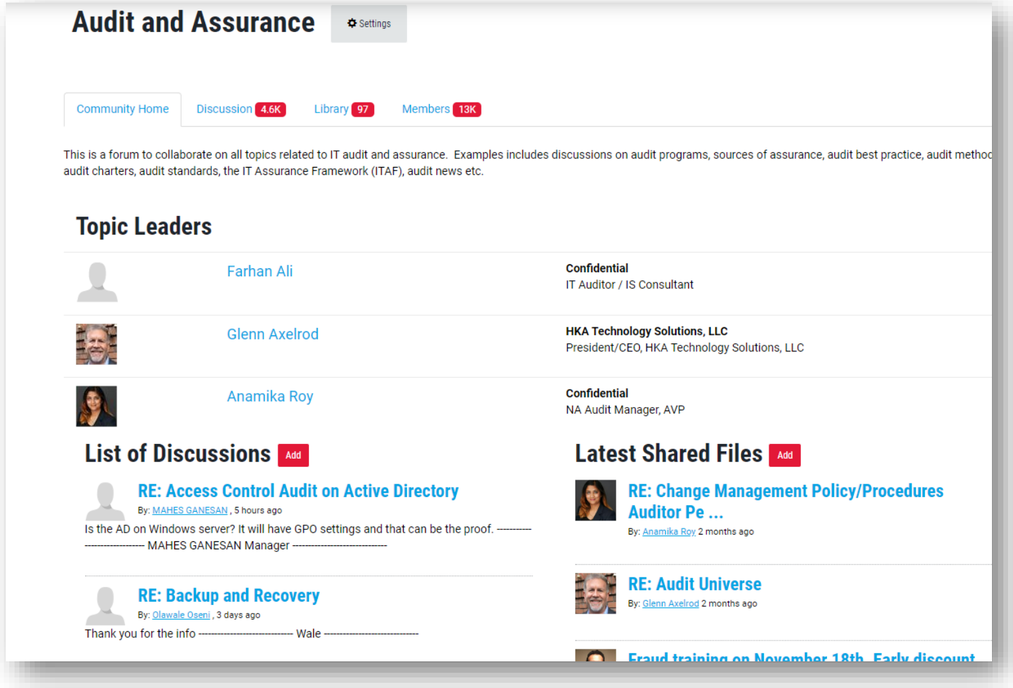
SheLeadsTech

Join

SheLeadsTech is a program from One In Tech, an ISACA Foundation. Join people of all genders in this global online community to discuss strategies that provide women the support and action they need to grow their careers and lead within the technology industry.

Discussions 2.3K | Libraries 37 | Members 1.4K

last person joined an hour ago



Thank you

twitter: gataya
Linked-in: ataya
gataya@solvay.edu

CYBER SECURITY COALITION.be

Solvay Brussels School
Executive Education

ATAYA&PARTNERS

Turning Audit into Enablement

Anatomy of an Audit Assignment

Kelly Hogan

Kelly Hogan
CISA, CIA, QAR-Accredited

- Over 25 years providing management and consulting advice on techniques for internal audit, risk management, control assessment and improvement, and written and oral communication
- Audits of financial, operational and information technology processes
- Previous head auditor of MasterCard Europe
- Since October 2006, provide consulting and training, primarily on audit topics and communication techniques, for individuals and audit departments of major multi-national organisations

An internal auditor?

About two years ago, Richard Chambers, President and CEO of the Institute of Internal Auditors (IIA) posted the following item on LinkedIn about internal auditors:

The next time someone asks:

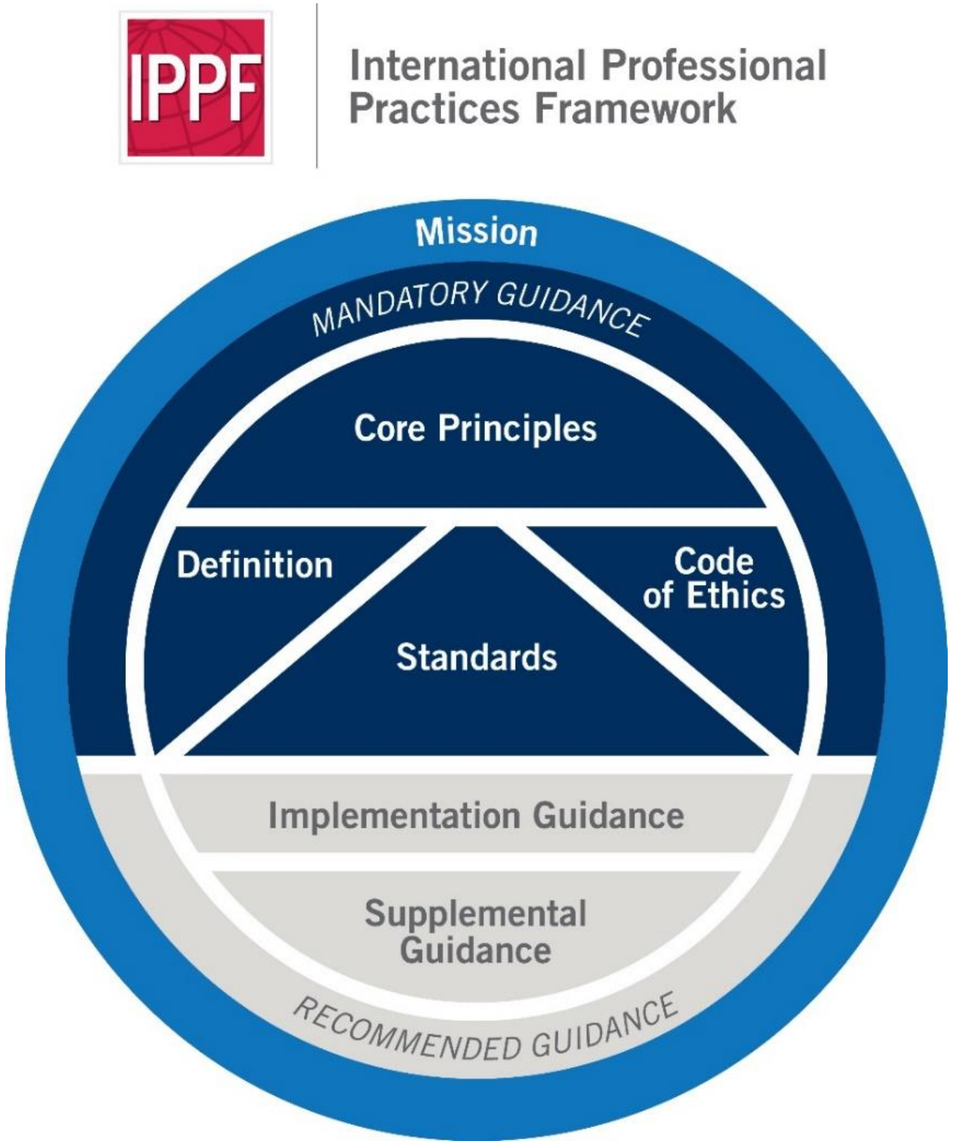
- *I am an internal auditor!*
- *I serve my organization to protect and enhance its value.*
- *I model integrity, objectivity, confidentiality, and competency every day.*
- *I improve risk management, internal controls, and governance in my organization.*
- *I follow The IIA's International Standards when providing assurance and advice.*
- *I am respected and admired, because I am a guardian of trust!*

Definition of Internal Audit (IIA)

Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

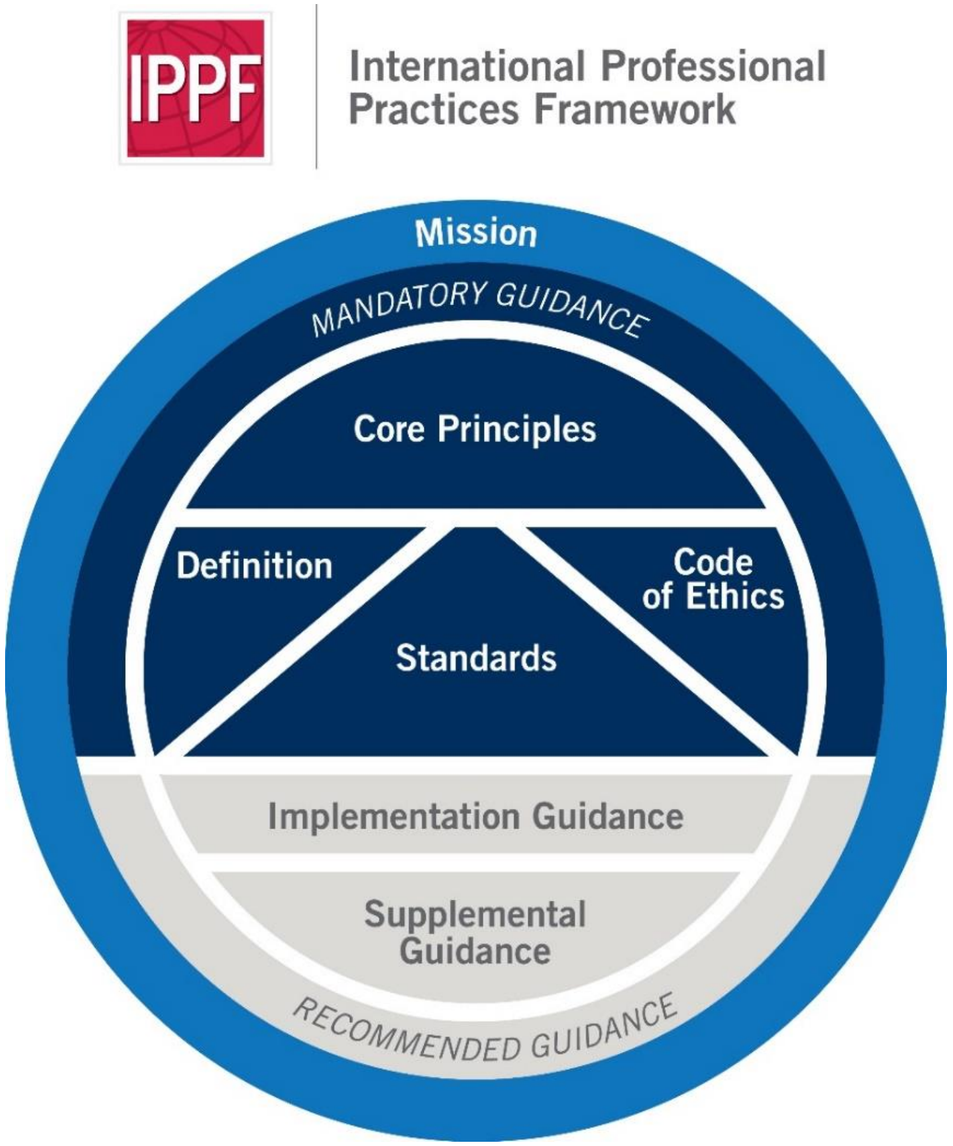
Internal audit framework

The IPPF is the conceptual framework that organizes authoritative guidance by The Institute of Internal Auditors (IIA).



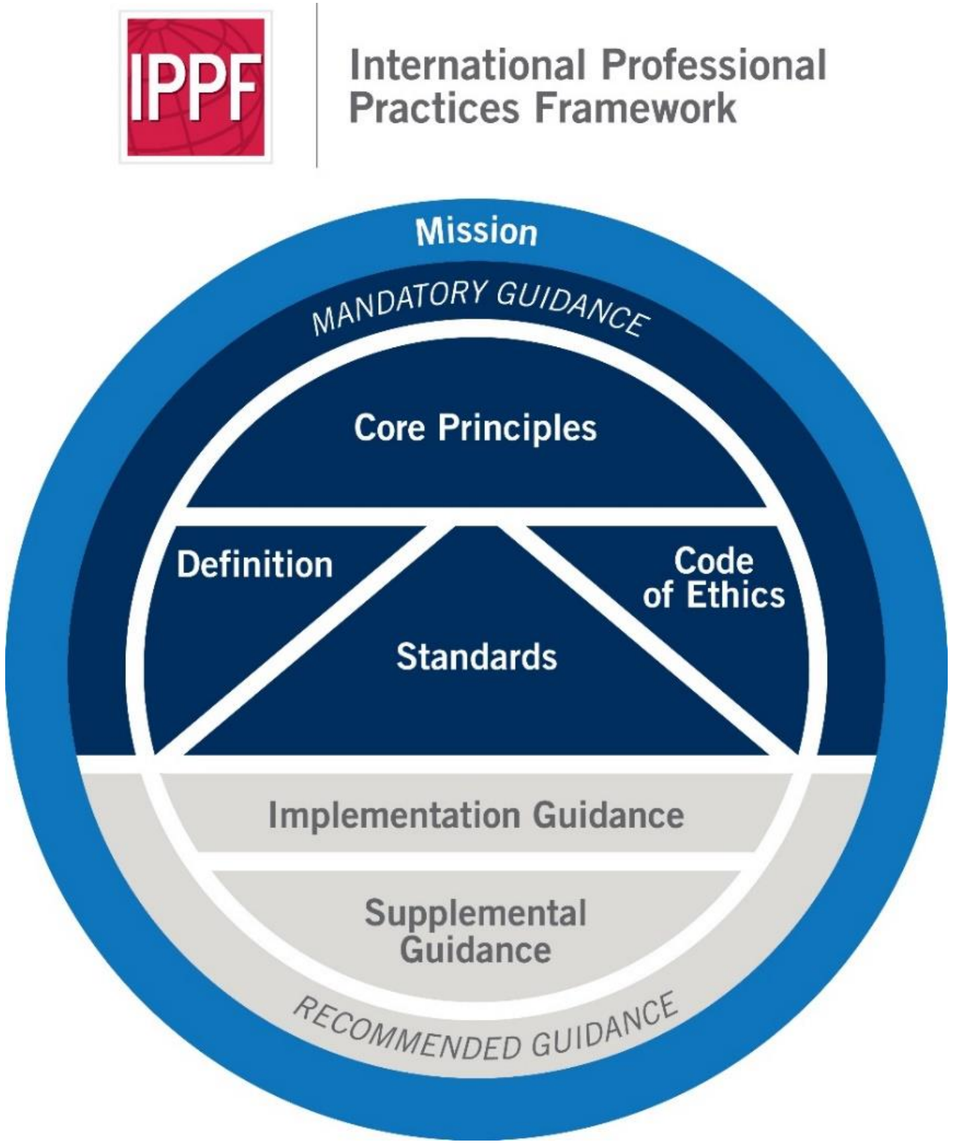
IIA Attribute standards

- 1000 Purpose, Authority and Responsibility
- 1100 Independence and Objectivity
- 1200 Proficiency and Due Professional Care
- 1300 Quality Assurance and Improvement Program



IIA Performance standards

- 2000 Managing the Internal Audit Activity
- 2100 Nature of work
- **2200 Engagement planning**
- **2300 Performing the engagement**
- **2400 Communicating results**
- 2500 Monitoring progress
- 2600 Communicating the acceptance of risks



Types of IT audit work

- Support for financial or operational audits
- General Controls audits
- Application Controls audits (often with operational auditors)
- Project audits
- Technical audits
- Consulting reviews

The IIA’s Audit Model

Planning – basic steps

- Conduct preliminary summary
- Determine initial objectives and scope
- Determine an audit budget and schedule
- Conduct opening meeting
- Hold walk-throughs and document processes (narratives and flow-charts)
- Develop a risk and control matrix (RCM)
- Gain agreement on objectives, scope, risks and timing with auditee

Note: These steps may or may not be done in the order stated.

Planning – objectives

Objectives must be established for each engagement. They can be general or specific.

- Review (assess, verify) whether controls have been designed to…
- Determine whether compliance has been achieved …
- Evaluate …

The objectives of the audit are to evaluate the design and effectiveness of risk management and internal controls related to billing and collections, and to determine the overall degree of compliance with applicable data protection and financial reporting regulations.

The objective of the audit is to assess the progress in addressing outstanding issues related to handling of security incidents.

Planning – scope

The established scope must be sufficient to achieve the objectives of the engagement. The scope must mention what is covered:

- Activity
- Process
- Department
- Product
- Contract
- Application

The scope of the audit includes all cart production operations at the Brussels and Antwerp facilities. The scope does not include wheel selection, which will be reviewed in a separate supplier audit in 20XX.

Planning – risk and control matrix (RCM) (1/4)

1	2	3	4	5	6
Objective/ Key Activity	Risk	Risk Level (H, M, L)	Control	Controls Sufficient?	Audit Test

Planning – RCM risks (2/4)

Risk
The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.

(IIA Standards – Glossary)

What could happen that would prevent or delay the business from meeting its objectives?

Planning – RCM controls (3/4)

Control
Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved.

Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved.

(Source: IIA Standards – Glossary)

Planning – RCM work program (4/4)

- Highlight control design deficiencies
- Determine which controls will be tested
- Develop the audit program
- Obtain supervisor review/approval

1	2	3	4	5	6
Objective/ Key Activity	Risk	Risk Level (H, M, L)	Control	Controls Sufficient?	Audit Test

Planning – deliverables to auditee

- Engagement Letter:
  - audit objectives and audit scope
  - key risk information
  - departments involved, key persons
  - timing
  - planned audit activities
- Opening Meeting
- RCM (less often)

The IIA's Audit Model

Performing – main tasks

- Gather evidence (Testing/Interviews)
- Document results
- Confirm facts
- Conclude on results
- Obtain supervisor review/approval
- Share information/gain agreement

Performing – types of evidence

- Physical
- Testimonial
- Documentary
  - External
  - Internal
- Analytical

Performing – rules of evidence

- **Sufficient** information is factual, adequate, and convincing so that a prudent, informed person would reach the same conclusions as the assurance provider.
- **Reliable** information is the best attainable information through the use of appropriate engagement techniques.
- **Relevant** information supports engagement observations and recommendations and is consistent with the objectives for the engagement.
- **Useful** information helps the organization meet its goals.

Source: IIA Standards

Performing – audit findings

- Criteria
- Condition
- Cause
- Consequence
- Corrective action

Review the facts and identify these five components during fieldwork.

Performing – deliverables to auditee

- Regular status meetings
- Initial finding details
- Closing meeting
  - Expected reportable findings

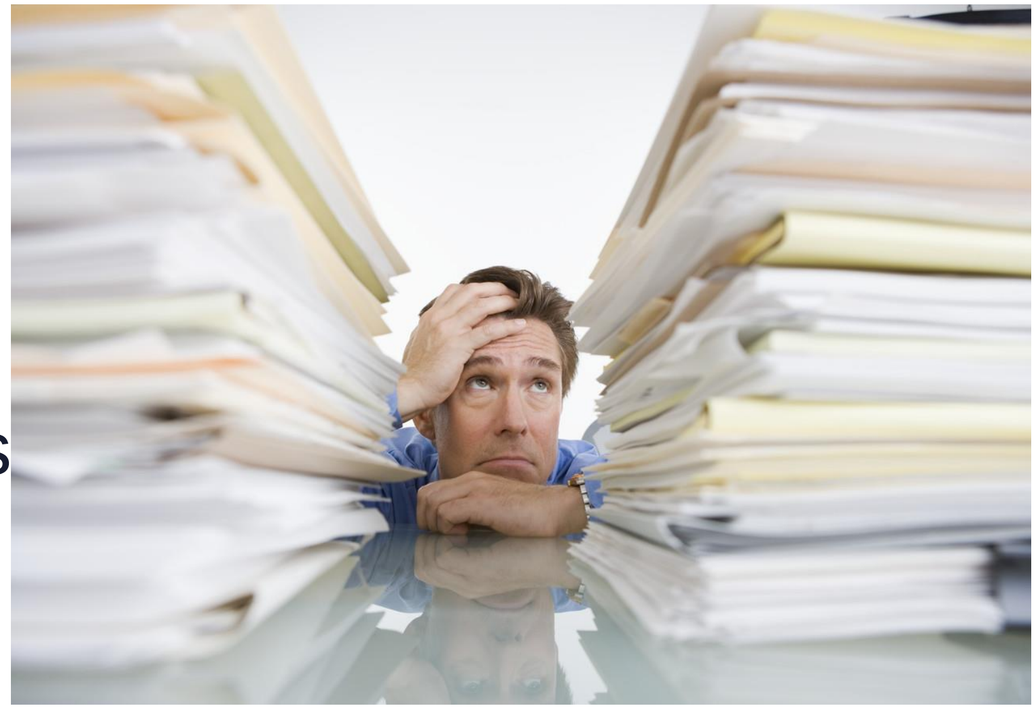
The IIA’s Audit Model

Communicating – main tasks

- Produce draft report
- Obtain supervisor review/approval
- Obtain comments on draft report
- Hold exit meeting
- Issue final report

Communicating – final report audience

Who reads audit reports?



- Audit clients (auditees)
- Senior management and executives
- Audit Committee and board members
- External auditors
- Regulators
- Internal auditors
- Customers (sometimes)

Communicating – typical audit report structure

1. Rating (if used)
2. Overall opinion
3. Detailed findings (possibly with ratings)
4. Business background information
5. Scope and objectives

✓ Use a table of contents
✓ Use appendices for additional material

Communicating – audit findings

What makes a good audit finding?

- Concisely describes the problem
- Conveys the reason for concern
- Addresses the reason for the problem
- Describes how the problem will (or should) be fixed

Communicating – corrective actions

Recommendations

- Describe ‘who should do what’ to fix the problem
- Require a management comment or response
- Leave a reader confused or frustrated if the management response is anything but ‘yes, we will’

Management Action Plans

- Describe ‘who will do what’ to fix the problem
- Require auditor to get agreement from management for all audit comments
- Give readers an immediate answer about how the audit comment will be addressed

Communicating – overall opinion

- Communicates key information about the audit results that an executive needs to know
- Describes how well (or not) risk is being managed for the business process or function that was audited
- Explains or justifies the rating, if one is given
- Provides a balanced view of the situation
- If necessary, motivates action

Communicating – deliverables to auditee

- Draft report for review and comment (factual accuracy, tone, corrective actions)
- Exit meeting
- Final report
- Customer survey

The IIA’s Audit Model

Monitoring – Main Tasks

- Identify action owners
- Report on outstanding actions and due dates
- Follow up on status of actions
- Close actions or escalate

Anatomy of an audit

Testwork – Use the arms and hands to reach – dig into the subject

Planning – Use the brain to get organised and work smart – analyse first and then focus on what matters

Interviews – Use the heart to connect with auditees and trunk to support findings

Reporting – Stand up straight on the legs and feet to communicate changes and walk into a better solution

CYBER SECURITY COALITION.be

ISACA Belgium Chapter

Solvay Brussels School Economics & Management

Thank you