MACFIN
MANAGEMENT CONSULTANTS

Università degli Studi di Roma "Tor Vergata"

IT risks and controls

2022

MACFIN Group

Let me introduce myself

MACFIN Group 30 YEARS

Alessandro Salibra Bove
Partner

- Shareholder and board member of MACFIN
- Certified CISA, CISM, CGEIT, CRISC, ISO 27001 Lead Auditor and ITIL Foundation. Member of AIIA and ISACA
- IT, Risk & Controls team

linkedin.com/in/alessandrosalibrabove/

Agenda

I – IT GOVERNANCE

IT evolution, objectives, roles and process model of an IT governance framework

II – IT RISK MANAGEMENT

Risk context, key elements of an IT Risk management framework, risk and measure examples

III – IT AUDIT CASE STUDY

Approach, planning and results of a real IT audit activity

Section I – IT GOVERNANCE

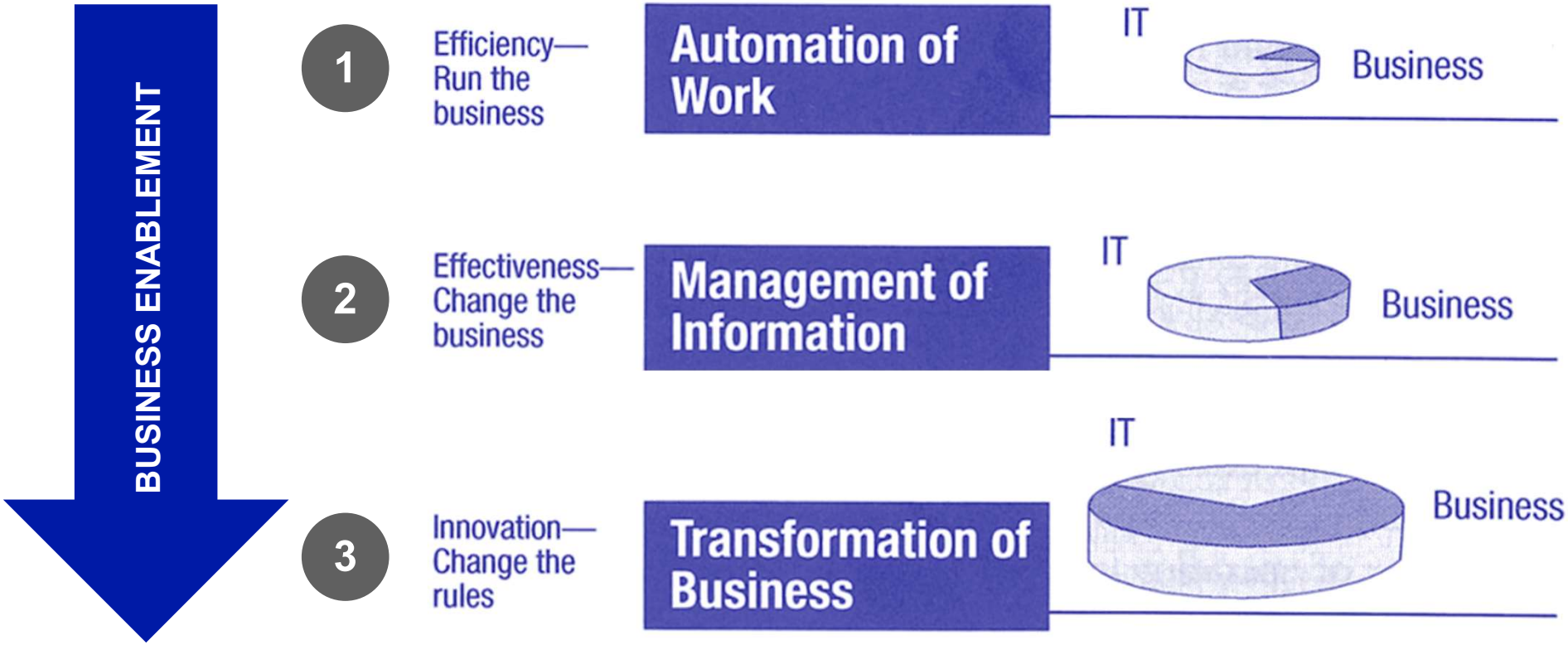
1. Main references adopted
2. IT evolution
3. IT governance definition and objectives
4. Governance enablers
5. Governance roles
6. Process reference model

IT governance

Main references adopted

IT governance

IT evolution



IT governance

Why IT Governance?

1. High-quality information
2. Business value
3. Operational excellence
4. IT-related risk
5. Cost of IT
6. Compliance

MACFIN
MANAGEMENT CONSULTANTS

IT governance

ISACA®
Trust in, and value from, information systems

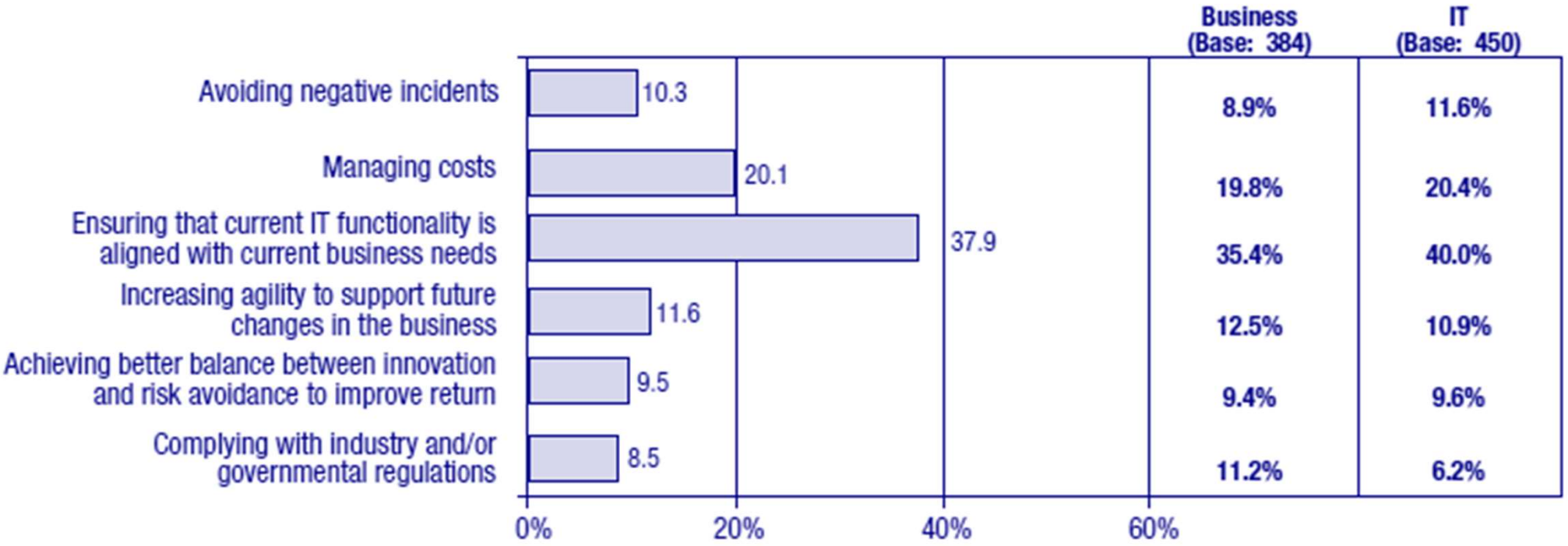
*"… the **responsibility of the board** of directors and executive management. It is an **integral part of entrprise governance** and consist of the leadership and organisational structures and processes that **ensure that the organisation's IT sustains and extends the organisation's strategies** and objectives.»*

MACFIN
MANAGEMENT CONSULTANTS

IT governance

«2. The management body should ensure that financial institutions have ***adequate internal governance and internal control framework in place for their ICT and security risks****. The management body should set clear roles and responsibilities for ICT functions, information security risk management, and business continuity […]»*

Drivers for IT Governance Activities



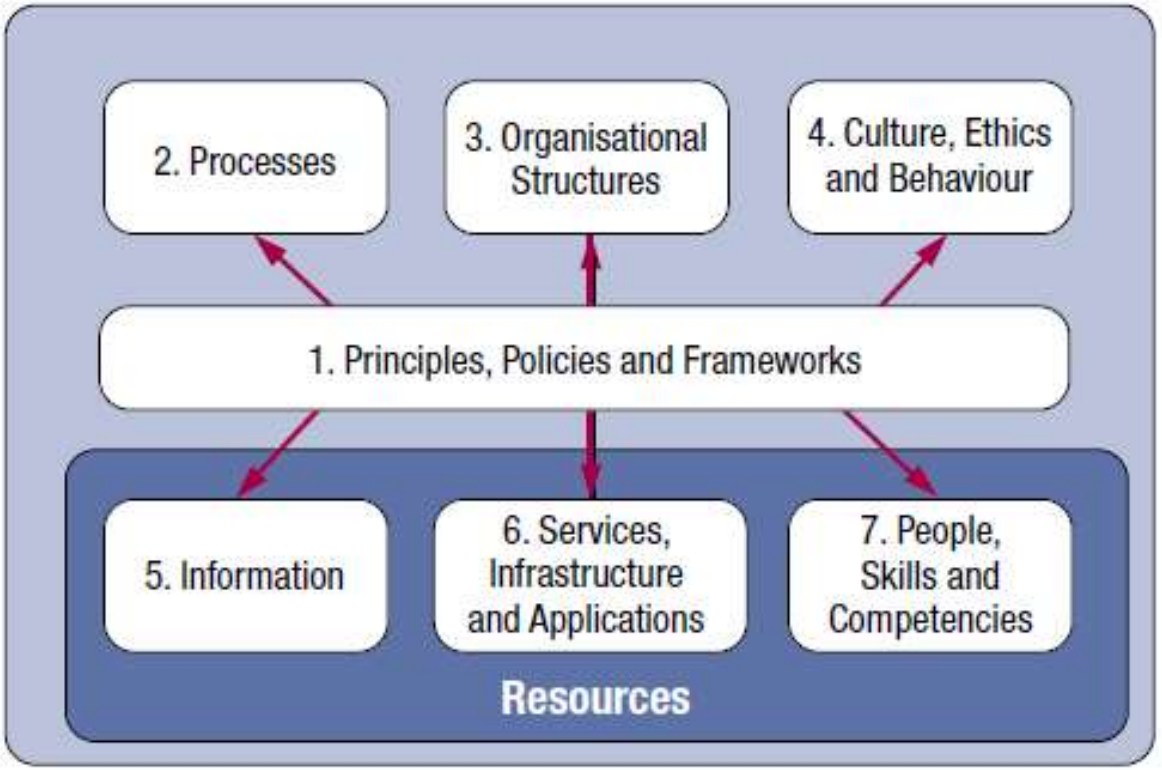
ITGI - Global Status Report on the Governance of Enterprise IT

COBIT
AN ISACA® FRAMEWORK

Governance objective

COBIT
AN ISACA® FRAMEWORK

Governance enablers



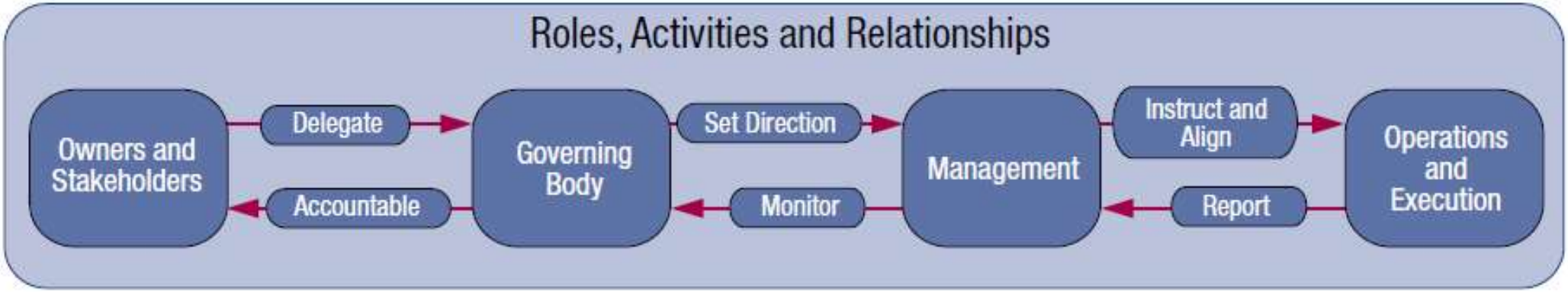
Governance enablers

«15. Financial institutions should identify, establish and maintain updated ***mapping of their business functions, roles and supporting processes*** *to identify the importance of each and their interdependencies related to ICT and security risks.*

16. In addition, financial institutions should identify, establish and maintain updated mapping of the ***information assets supporting their business functions and supporting processes, such as ICT systems, staff, contractors, third parties and dependencies*** *on other internal and external systems and processes […]»*

COBIT
AN ISACA® FRAMEWORK

Governance roles

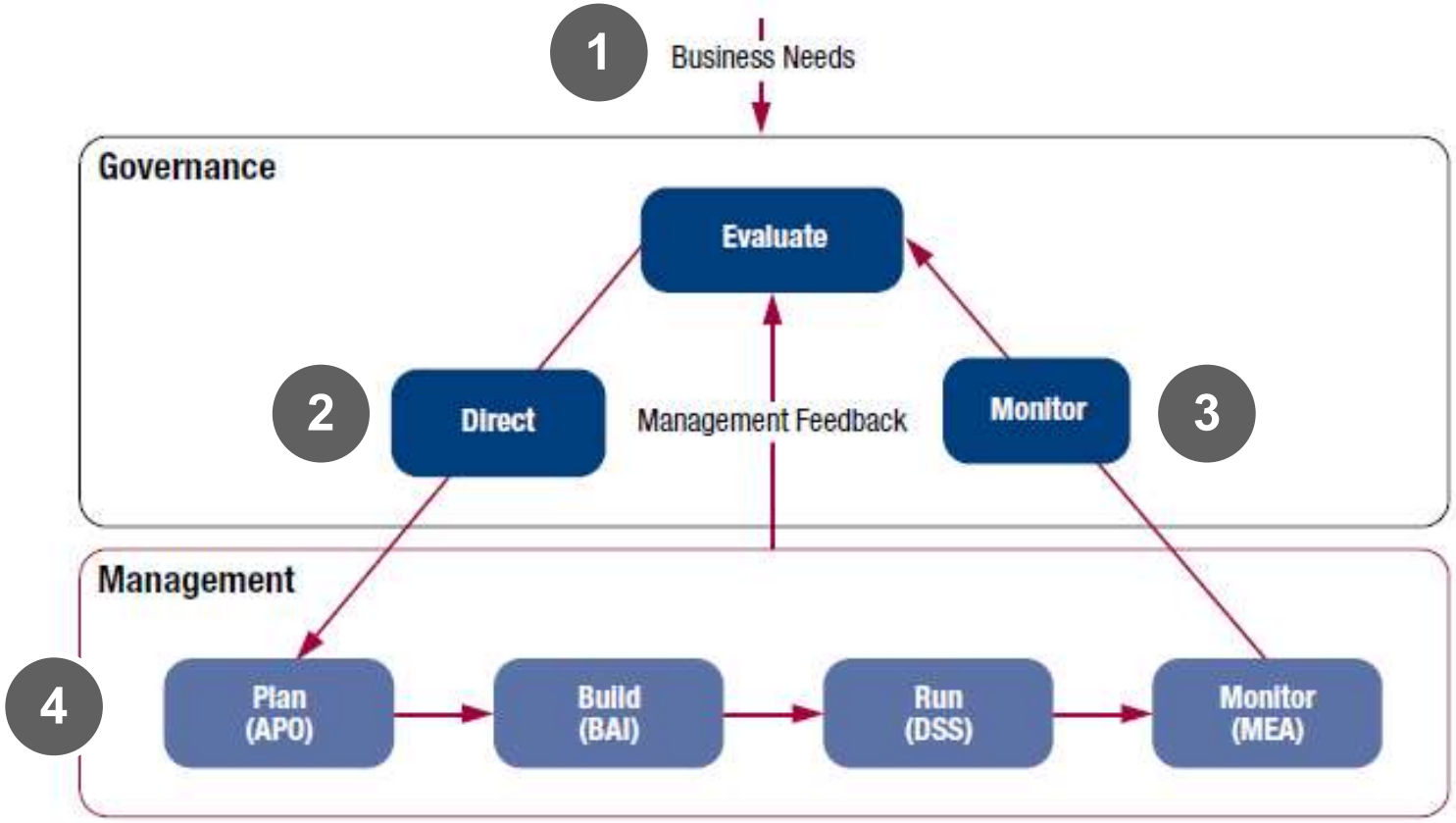


Governance roles

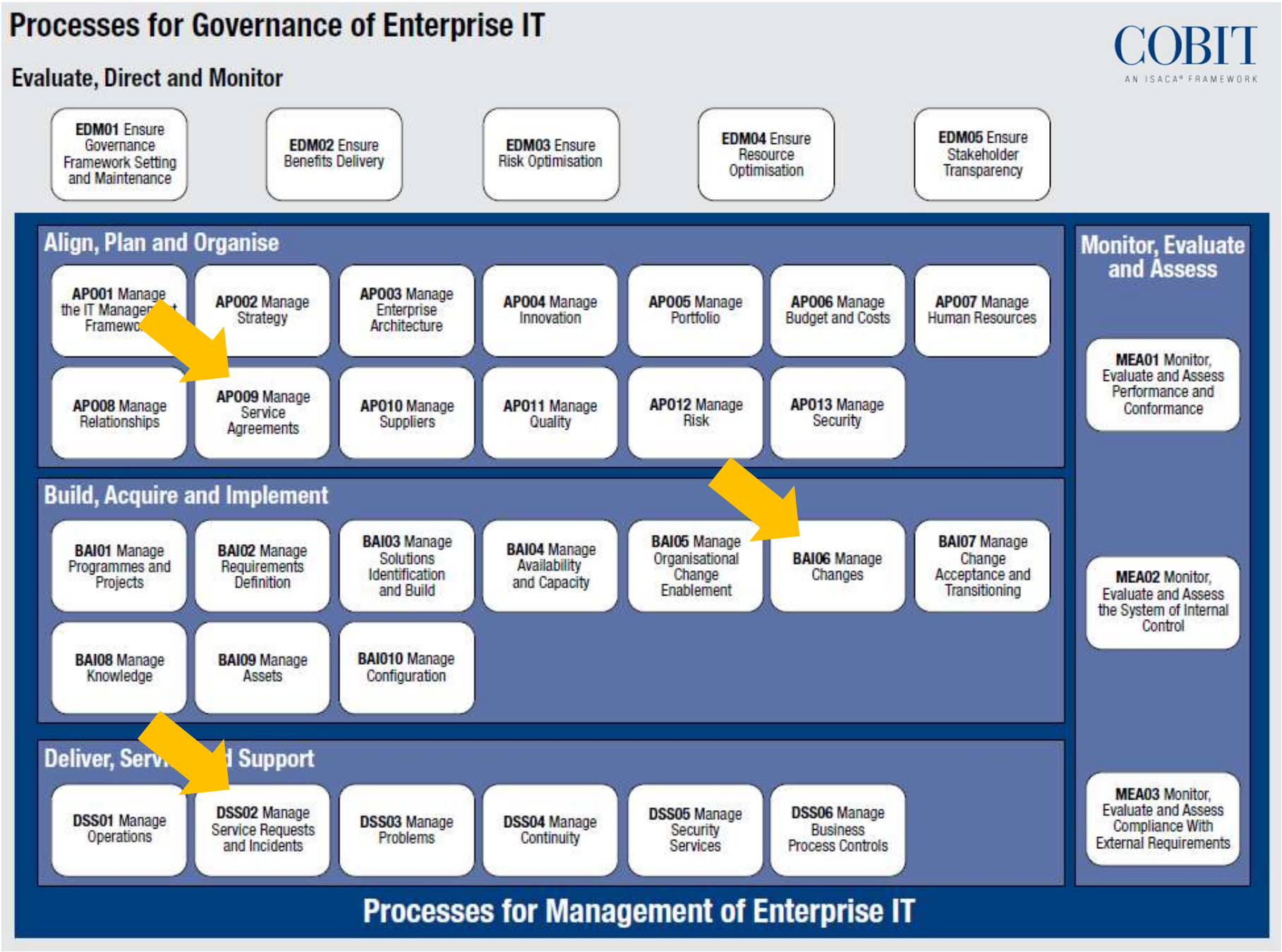
*«4. The **management body has overall accountability for setting, approving and overseeing the implementation of financial institutions' ICT strategy** as part of their overall business strategy as well as for the establishment of an effective risk management framework for ICT and security risks.»*

COBIT
AN ISACA® FRAMEWORK

Process reference model



IT governance



Sample

DSS02 Manage Service Requests and Incidents — COBIT	Area: Management Domain: Deliver, Service and Support
Process Description Provide timely and effective response to user requests and resolution of all types of incidents. Restore normal service; record and fulfil user requests; and record, investigate, diagnose, escalate and resolve incidents.	
Process Purpose Statement Achieve increased productivity and minimise disruptions through quick resolution of user queries and incidents.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
04 Managed IT-related business risk	• Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment • Number of significant IT-related incidents that were not identified in risk assessment • Percent of enterprise risk assessments including IT-related risk • Frequency of update of risk profile
07 Delivery of IT services in line with business requirements	• Number of business disruptions due to IT service incidents • Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels • Percent of users satisfied with the quality of IT service delivery
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. IT-related services are available for use.	• Number and percent of incidents causing disruption to business-critical processes • Mean time between incidents according to IT-enabled service
2. Incidents are resolved according to agreed-on service levels.	• Percent of incidents resolved within an agreed-on/acceptable period of time
3. Service requests are dealt with according to agreed-on service levels and to the satisfaction of users.	• Level of user satisfaction with service request fulfilment • Mean elapsed time for handling each type of service request

So, why COBIT ?

AN ISACA® FRAMEWORK

isaca.org/cobit

Section II – IT RISK MANAGEMENT

1. Key points of context
2. Risk / IT risk definitions
3. IT risk categories
4. Risk scenario structure and risk factors
5. Risk scenario and response examples

IT risk management

Key points of context

1. IT as a key element for creating value
2. Regulations govern information technology
3. Growing need to manage risks related to IT
4. IT risk management requires to address the full scope of strategic impacts

Risk / IT risk definitions

ISO International Organization for Standardization

RISK

Risk is the combination of the probability of an event and its consequence. Consequences are that enterprise objectives are not met.

COBIT

INFORMATION and related Technologies (IT) RISK

IT risk is a business risk, specifically, the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise.

EBA European Banking Authority

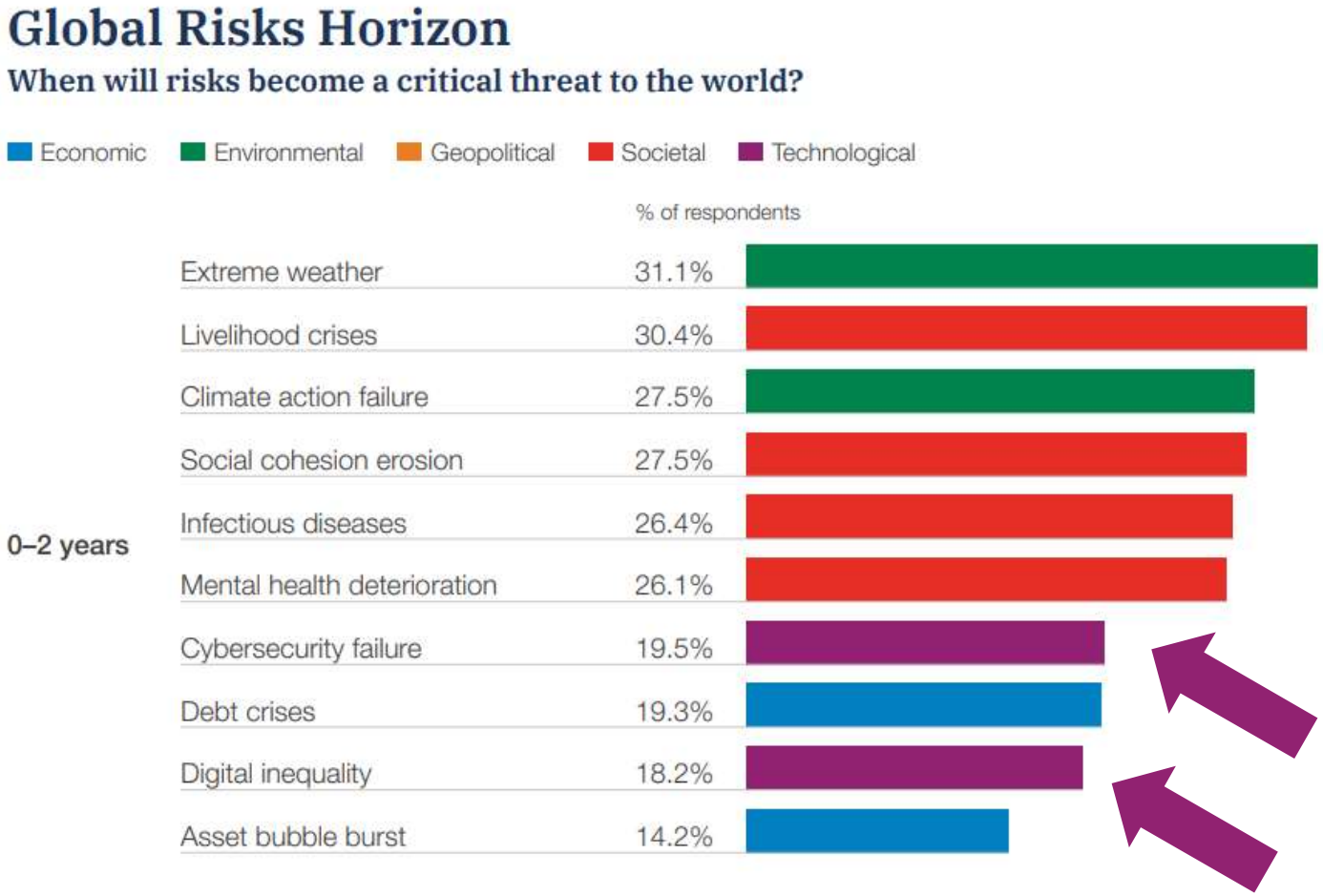
ICT and security risk

Risk of loss due to breach of confidentiality, failure of integrity of systems and data, inappropriateness or unavailability of systems and data or inability to change information technology (IT) within a reasonable time and with reasonable costs when the environment or business requirements change (i.e. agility).

IT risk management

Global Risks Report

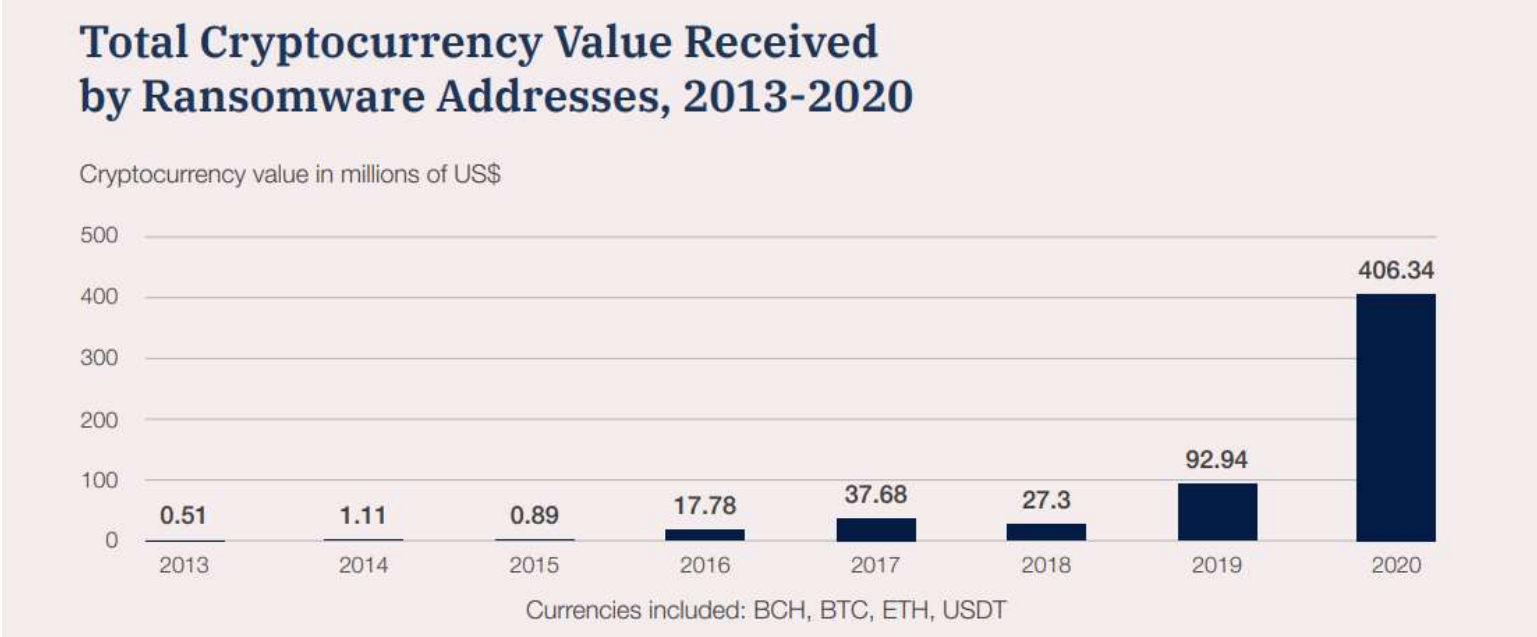
The Global Risks Landscape



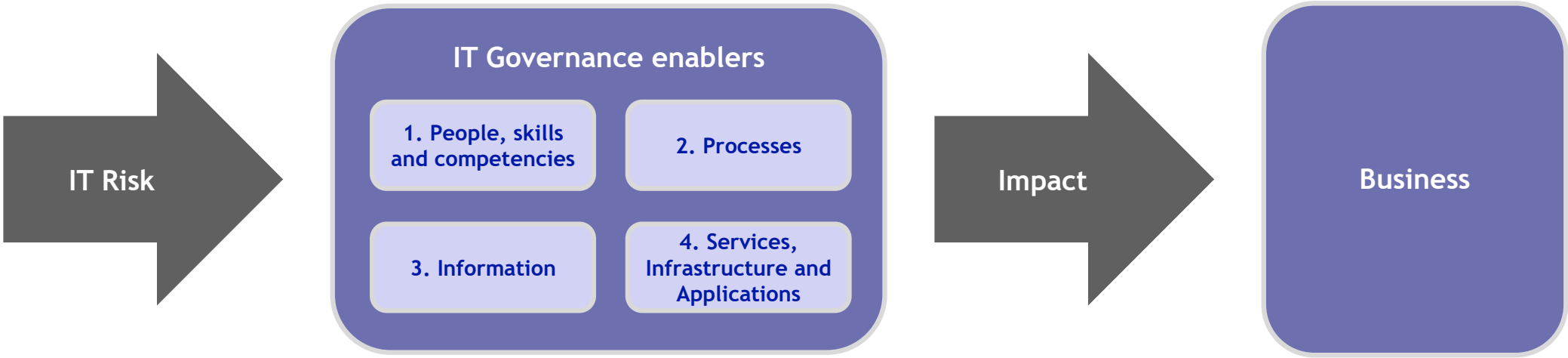
IT risk management

Global Risks Report

The Global Risks Landscape



More in particular, what is an IT Risk?



MACFIN
MANAGEMENT CONSULTANTS

IT risk management

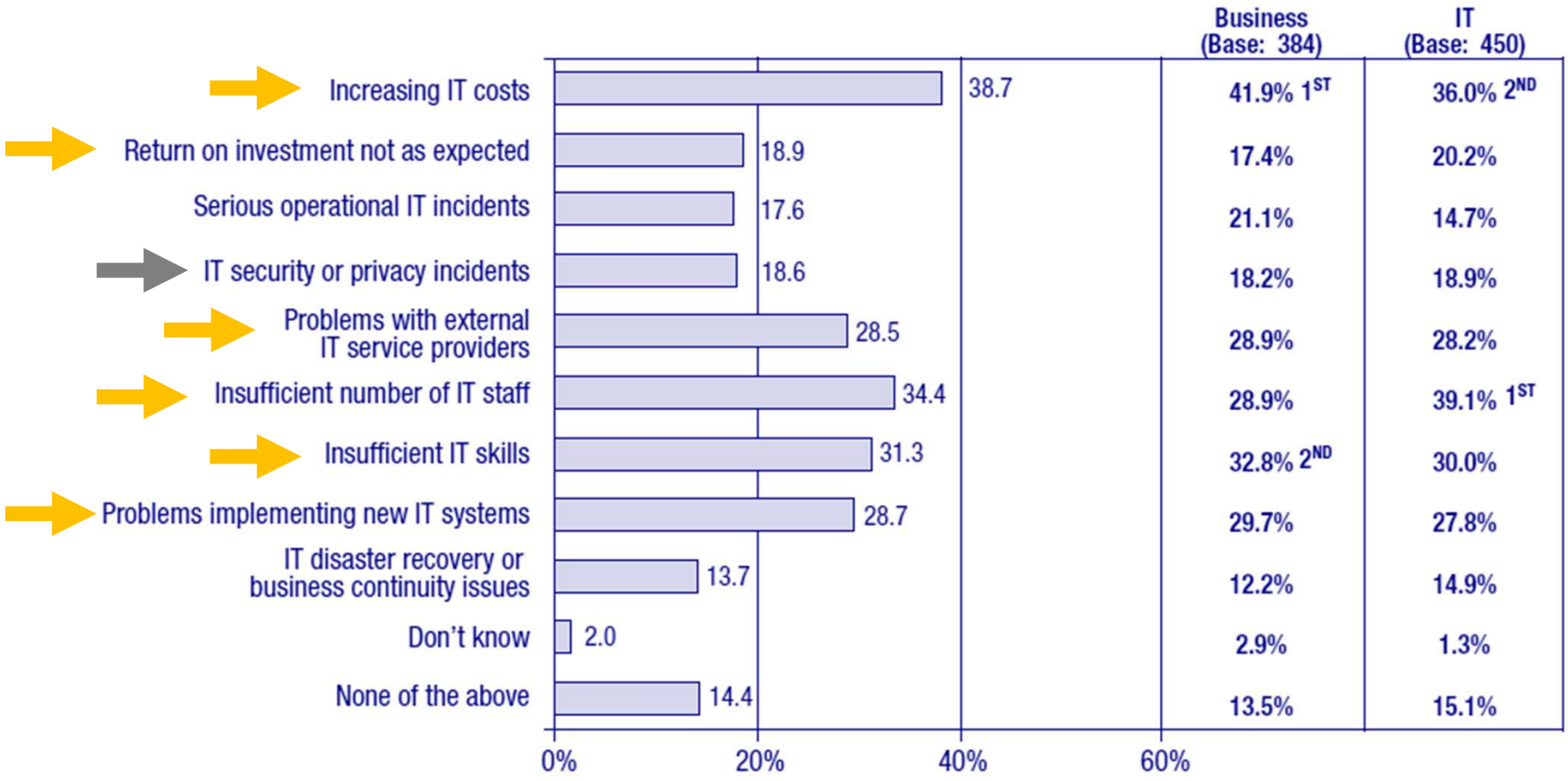
COBIT
AN ISACA® FRAMEWORK

IT risk categories

1. IT Benefit / Value Enablement
2. IT Programme and Project Delivery
3. IT Operations and Service Delivery

IT risk management

IT-related Issues Experienced in the Past 12 Months



ITGI - Global Status Report on the Governance of Enterprise IT

So, how can I assess IT risks?

Risk assessment process

ICT and security risk management framework

«10. Financial institutions should identify and manage their ICT and security risks. […] ensure that ***all risks are identified, analysed, measured, monitored, managed, reported and kept within the limits*** *of the financial institution's risk appetite […]*

11. Financial institutions should ***assign the responsibility for managing and overseeing ICT and security risks to a control function*** *[…] ensure the* ***independence and objectivity*** *of this control function by appropriately* ***segregating it from ICT operations processes****. […]»*

COBIT
AN ISACA® FRAMEWORK

Risk scenario structure

COBIT

Risk scenario examples from COBIT

Sample

Risk sub-Category	Risk scenario	Cobit Ref
1. Projects portfolio establishment and maintenance	There is duplication between initiatives.	0102
2. Programme/projects life cycle management	There is an IT project budget overrun.	0202
3. IT investment decision making	The wrong software, in terms of cost, performance, features, compatibility, etc., is selected for implementation.	0302
4. IT expertise and skills	There is a lack of or mismatched IT-related skills within IT, e.g., due to new technologies.	0401
5. Staff operations (error and malicious intent)	Hardware components were configured erroneously.	0508
6. Information (data breach: damage, leakage and access)	Portable media containing sensitive data (CD, USB drives, portable disks, etc.) is lost/disclosed.	0603
7. Architecture (architectural vision and design)	The enterprise architecture is complex and inflexible, obstructing further evolution and expansion leading to missed business opportunities.	0701
8. Infrastructure	The systems cannot handle transaction volumes when user volumes increase.	0802
9. Software	Intentional modification of software leading to wrong data or fraudulent actions.	0906

COBIT
AN ISACA® FRAMEWORK

Risk scenario examples from COBIT

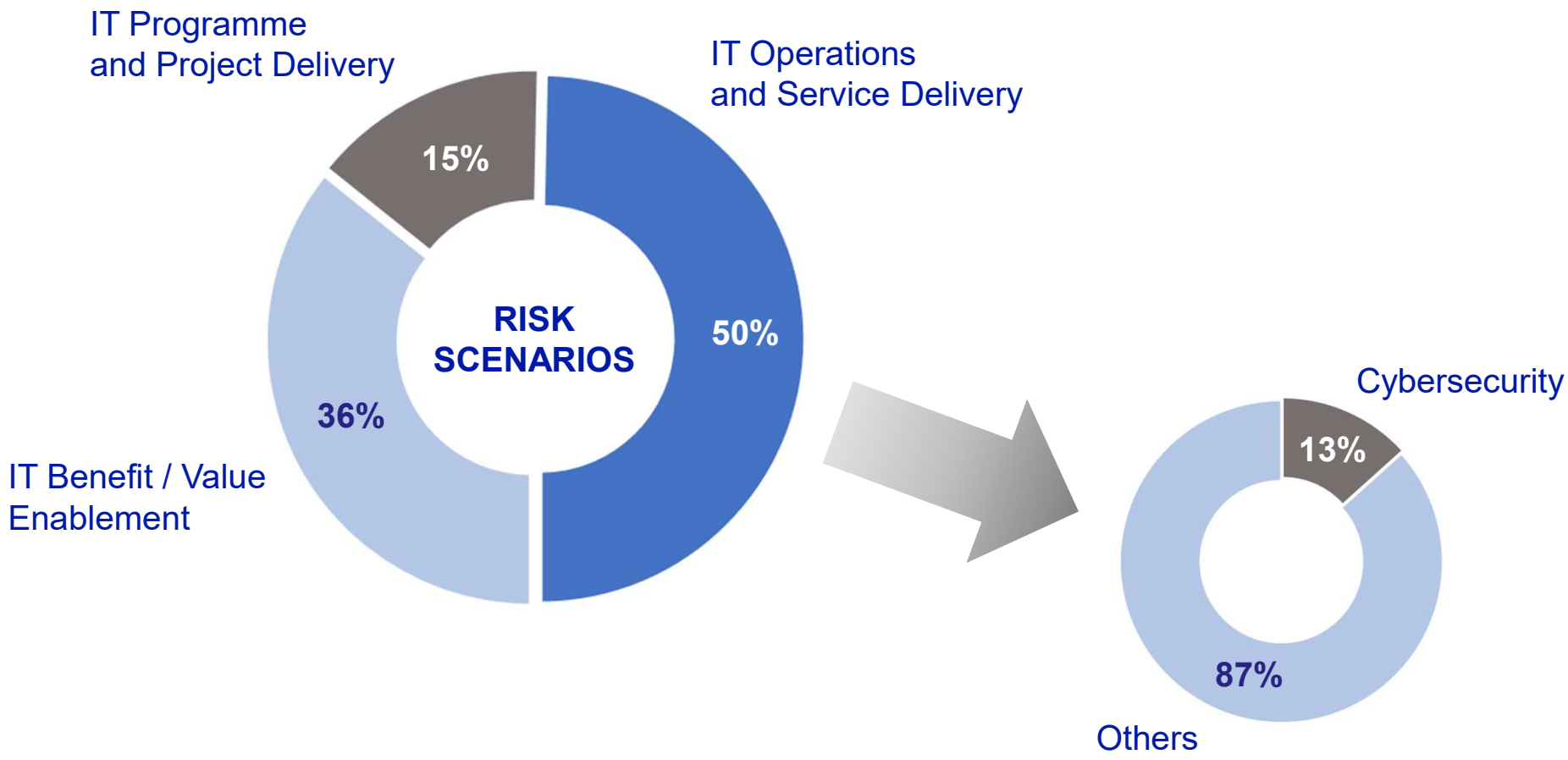
Sample

Risk sub-Category	Risk scenario	Cobit Ref
10. Business ownership of IT	Business does not assume accountability over those IT areas it should, e.g., functional requirements, development priorities, assessing opportunities through new technologies.	1001
11. Supplier selection/performance, contractual compliance, termination of service and transfer	Support and services delivered by vendors are inadequate and not in line with the SLA.	1103
12. Regulatory compliance	There is non-compliance with regulations, e.g., privacy, accounting, manufacturing.	1201
13. Infrastructure theft or destruction	Destruction of the data centre (sabotage, etc.) occurs.	1403
14. Malware	Regularly, there is infection of laptops with malware.	1502
15. Logical attacks	There is a service interruption due to denial-of-service attack.	1602
16. Industrial action	Facilities and building are not accessible because of a labour union strike.	1701
17. Acts of nature	There is flooding	1905

IT risk management

COBIT
AN ISACA® FRAMEWORK

Risk scenarios by category



Risk response examples from COBIT

Sample

Risk sub-Category	Risk responses (Cobit Processes)	Cobit Ref
1. Projects portfolio establishment and maintenance	Prioritise resource allocation.	APO06.02
2. Programme/projects life cycle management	Maintain a standard approach for programme and project management.	BAI01.01
3. IT investment decision making	Manage stakeholder engagement.	BAI01.03
4. IT expertise and skills	Plan and track the usage of IT and business human resources.	APO07.05
5. Staff operations (error and malicious intent)	Manage contract staff.	APO07.06
6. Information (data breach: damage, leakage and access)	Ensure traceability of Information events and accountabilities.	DSS06.05
7. Architecture (architectural vision and design)	Define reference architecture.	APO03.02
8. Infrastructure	Monitor and scan the technology environment.	APO04.03
9. Software	Evaluate, prioritise and authorise change requests.	BAI06.01

COBIT

Risk response examples from COBIT

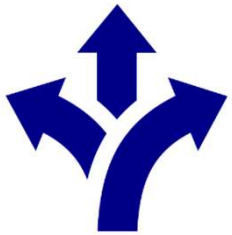
Sample

Risk Category	Risk responses (Cobit Processes)	Cobit Ref
10. Business ownership of IT	Monitor and report service levels.	APO09.04
11. Supplier selection/performance, contractual compliance, termination of service and transfer	Monitor supplier performance and compliance.	APO10.05
12. Regulatory compliance	Identify external compliance requirements.	MEA03.01
13. Infrastructure theft or destruction	Manage physical access to IT assets.	DSS05.05
14. Malware	Monitor the infrastructure for security-related events.	DSS05.07
15. Logical attacks	Monitor IT infrastructure.	DSS01.03
16. Industrial action	Identify key IT personnel.	APO07.02
17. Acts of nature	Exercise, test and review the Business Continuity Plan.	DSS04.04

Section III – IT AUDIT CASE STUDY

1. IT audit approach
2. Audit scope and planning
3. Risk assessment
4. Audit areas
5. Methods adopted
6. Audit report and improvement points
7. Key points

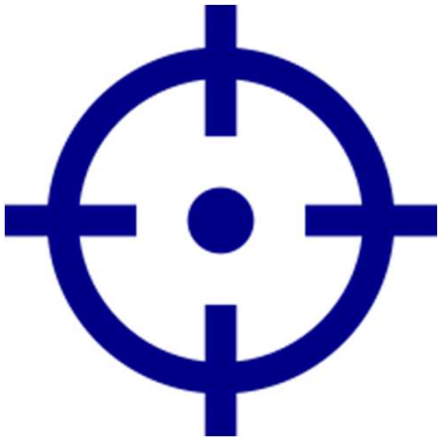
IT audit - Case study



IT audit approach

1. Overall analysis
2. Effective checks
3. Search of logic vulnerabilities

IT audit - Case study



Audit scope

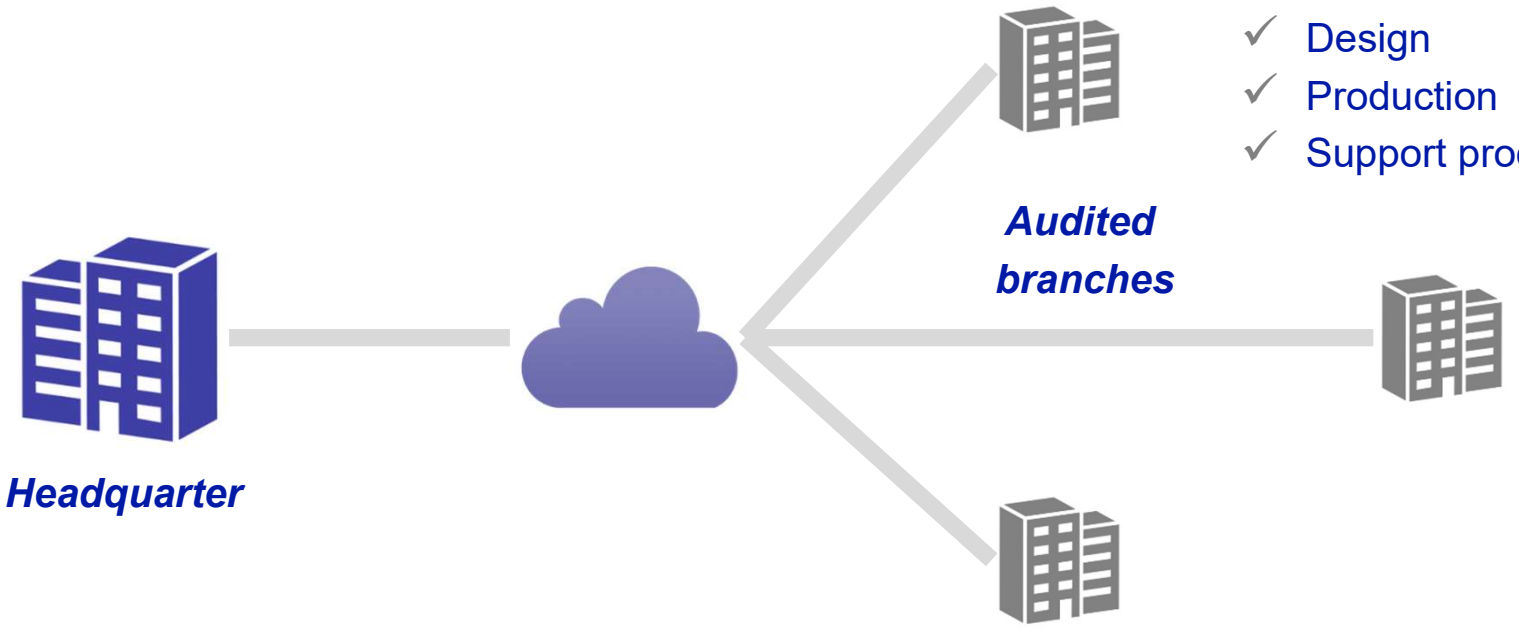
1. Main foreign branches of a leading company in the industrial sector
2. Company has 20 foreign branches on several continents

IT audit - Case study

Information system audited

Applications:

- ✓ Tenders
- ✓ Design
- ✓ Production
- ✓ Support processes



IT audit - Case study

Audit planning

1. Preliminary survey

- ✓ Documentation analysis
- ✓ Interviews

2. Risk assessment

- ✓ IT systems
- ✓ IT management processes

3. Audit plan

- ✓ Audit areas
- ✓ Checks

Risk assessment

PURPOSE

1. Identify and assess IT risk
2. Define the audit program

IT audit - Case study

Risk assessment

IT Risk assessment process

Taylor-made check-list

Audit support

Real-time results

IT audit - Case study

Risk assessment

Category	Risks	L	M	H
IT Architecture	The enterprise architecture is complex, obstructing further evolution and not supporting the business priorities			
IT expertise and skills	There is a lack in IT staff recruiting process			
	There are insufficient IT HR to cover the business requirements.			
	There is an overreliance on key IT staff			
	There are insufficient skills to cover the business requirements.			
Software	There is extensive use of end-user computing for important information (ex. Excel), leading to security deficiencies, inaccurate data or increasing costs			
	There is a lack in IT training/support/user's guide for new application software or software release			
Information management	Data are lost, inaccessible or corrupted (e.g. backup media is lost or backups are not checked for effectiveness; data are modified intentionally).			
IT Project Portfolio Management	There is a failure/overbudget/delay in IT project delivery			
	Competing resources are allocated and managed inefficiently and are misaligned to business priorities			

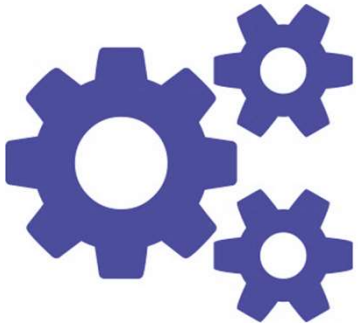
Risk assessment

- IT benefit/value enablement risk
- IT operations and service delivery risk
- IT programme and project delivery risk

Audit areas

Area	Cobit Ref
1. System administrators	DSS05.04
2. Management of users and authorisations	DSS05.04
3. Software licensing management	BAI09.05
4. Security of IT workstations	DSS05.03
5. Electronic signature	DSS05.06

IT audit - Case study



Methods adopted

1. Analysis of company regulations
2. Surveying practices and IT systems
3. Process walk-throughs
4. Verifying IT system

IT audit - Case study

Audit report

1. Methods used to plan and carry out the activities
2. Improvement points
3. Suggestions for action

SAMPLE

Scope 1. System Administrators

Audit results	The audits carried out on AdS (System Administrators) underlined as follows: • The contract documents do not clearly define: • the name of operative AdS; • the scope of activity of each AdS. • Some Administration accounts not registered to any name have been found; in particular, 4 collaborators acting as AdS use all the same account "Administrator". •The AdS have no restrictions as to the creation of password (minimum length of and characters forming the password).

Audits	Population/ Sample	Outcome / Significance	
In the contract documents: •Identification of operative AdS by name; •Scope of activity of each AdS.	Contract documents.	The subject-matter aspects are not defined in the contract documents.	Medium High
Existence of only name-registered administrator accounts in the centralized authentication system used at the branch-office (*local domain*).	List of users includes in the "AdS" authentication group of the local domain.	Based on the audit carried out in the *local domain* it appeared that 4 collaborators of the company acting as AdS use all the same account "Administrator«, contrarily to the provisions of the Policy governing the use of corporate information-technology systems.	Medium High

IT audit - Case study

Improvement points

1. Contractual definition of System Administrators
2. Use of shared folders
3. Inventory of software in use
4. Traceability of new user requests

Critical factors

1. Co-existence of local and central IT systems
2. Outsourced IT administration
3. Temporary nature of the production sites
4. Specific needs of each production site

DISCUSSION

Risk identification

Discussion

GDPR

*"In assessing the appropriate level of security account shall be taken in particular of the **risks that are presented by processing**, in particular from accidental or unlawful **destruction, loss, alteration, unauthorised disclosure** of, or access to **personal data** transmitted, stored or otherwise processed."*

Assessing the risk connected to personal data security – see a requirement of the EU General Data Protection Regulation – which are the risk scenarios to consider among the ones detailed in the following slide?

Discussion

GDPR

*"In assessing the appropriate level of security account shall be taken in particular of the **risks that are presented by processing**, in particular from accidental or unlawful **destruction, loss, alteration, unauthorised disclosure** of, or access to **personal data** transmitted, stored or otherwise processed."*

Risk Category	Risk scenario	Cobit Ref
1. Portfolio establishment and maintenance	There is duplication between initiatives.	0102
2. Programme/projects life cycle management	There is occasional late IT project delivery by an internal development department.	0203
3. IT investment decision making	Redundant software is purchased.	0304
4. IT expertise and skills	There is a lack of or mismatched IT-related skills within IT, e.g., due to new technologies.	0401
5. Staff operations (error and malicious intent)	Hardware components were configured erroneously.	0508
6. Information (data breach: damage, leakage and access)	Portable media containing sensitive data (CD, USB drives, portable disks, etc.) is lost/disclosed.	0603
7. Architecture (architectural vision and design)	There is a failure to adopt and exploit new infrastructure in a timely manner.	0703
8. Infrastructure	The systems cannot handle transaction volumes when user volumes increase.	0802

Which are the risk scenarios to consider?

Thank you!

Alessandro Salibra Bove

Partner

MACFIN Group
CONSULTING SERVICES

a.salibra@macfin-group.net

www.macfin-group.net