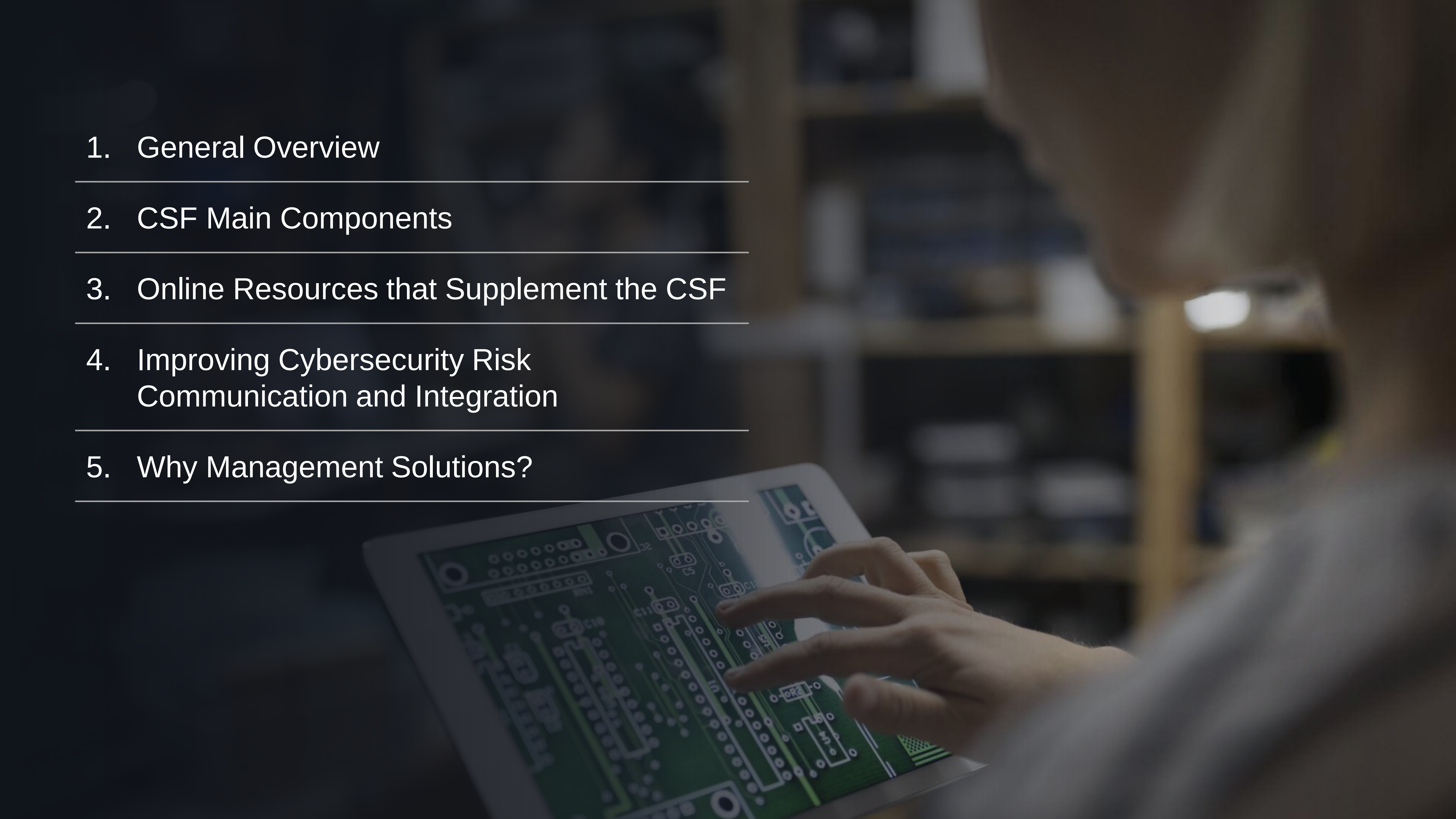
Cybersecurity Framework 2.0

NIST final version

Research & Development | www.managementsolutions.com | **April 2024**



1. General Overview
2. CSF Main Components
3. Online Resources that Supplement the CSF
4. Improving Cybersecurity Risk Communication and Integration
5. Why Management Solutions?

1 General Overview

Executive summary

The NIST Cybersecurity Framework (CSF) 2.0 is designed to help organizations of all sizes and sectors, including industry, government, academia, and nonprofit, to manage and reduce their cybersecurity risks

Context

- In October 2023, the NIST released a **draft version of the Cybersecurity Framework (CSF) 2.0**, a new version of a tool it first released in 2014 to help organizations understand, reduce and communicate about cybersecurity risk. The CSF is the result of a multi-year collaborative effort across industry, academia, and government in the United States and around the world.
- CSF 2.0 contains **new features** that highlight the importance of governance and supply chains. Special attention is paid to the Quick Start Guides (QSGs) to ensure that the CSF is relevant and readily accessible by smaller organizations as well as their larger counterparts.
- NIST now provides **Implementation Examples** and **Informative References**, which are available online and updated regularly.

Objectives

- The NIST CSF 2.0 **provides guidance** to industry, government agencies, and other organizations to manage cybersecurity risks.
- The CSF 2.0 **assists** organizations in managing cybersecurity risks with flexibility, providing accessible guidance for all levels.
- It **encourages** integration of cybersecurity with other enterprise risks and offers tools like Quick Start Guides (QSG).
- CSF 2.0 **focuses** on governance and supply chains, enabling swift implementation and adaptation to evolving threats.

Main content

CSF Main components	Core	Organizational Profiles	Tiers
Online resources that supplement the CSF	Informative References	Implementation examples	QSGs
Improving Cybersecurity Risk	Communication	Integration	

Access to Document

2 CSF Main Components

Core Functions

The CSF Core Functions are a set of six key actions that organize cybersecurity outcomes. These functions should be addressed concurrently and apply to all types of Information and Communications Technology (ICT) used by an organization and apply to all types of technology environments

Govern…

…Setting the **overall direction for cybersecurity** within the organization. This includes activities such as establishing a cybersecurity strategy, defining roles and responsibilities, and overseeing the implementation of the CSF.

Identity…

… Helping understanding cybersecurity risks by **identifying company's assets** (data, systems, people, etc.) **and the threats that could impact those assets.**

Protect…

…Helping implementing safeguards to protect assets from cybersecurity attacks. These safeguards can include firewalls, access controls, data encryption….

Detect…

… Helping detecting **cybersecurity attacks** that may be in progress. This includes activities such as **monitoring systems** for suspicious activity and analyzing logs for signs of intrusion.

Respond…

… Helping **responding to cybersecurity incidents that have occurred**. This includes activities such as containing the incident, mitigating the damage, and recovering from the attack.

Recover…

… Helping **restoring systems and data after a cybersecurity incident**. This includes activities such as restoring backups, repairing damaged systems, and resuming normal operations.

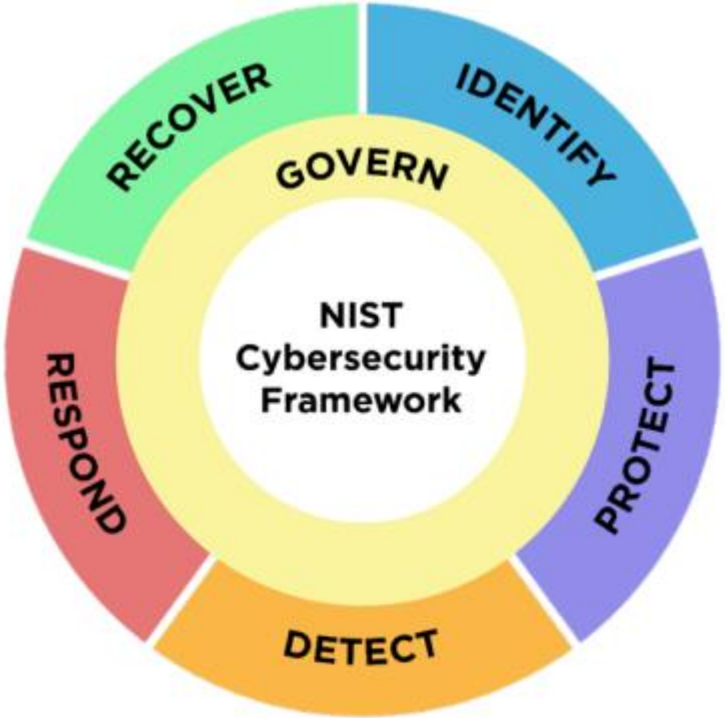


Fig. 2. CSF Functions

2 CSF Main Components
Profiles

Profiles are mechanisms for describing an organization's current and target cybersecurity posture in terms of the Core's outcomes, and used to understand, tailor, assess, prioritize, and communicate the Core's outcomes by considering an organization's mission objectives, stakeholder expectations, threat landscape, and requirements

Organizational Profile includes one or both of the following

Current profile

Specifies the Core **outcomes** that an organization is **currently achieving** and characterizes how or to what extent each outcome is being achieved

Target profile

Specifies the **desired outcomes** that an organization has **selected and prioritized** for achieving its cybersecurity risk management objectives

Community Profile

A **Community Profile** is a baseline of CSF outcomes that is created and published to address shared interests and goals among a number of organizations. A Community Profile is typically developed for a particular sector, subsector, technology, threat type, or other use case. An organization can use a Community Profile as the basis for its own Target Profile.

Steps for creating and using a CSF Organizational Profile

1 Scope the Organizational profile

Document the high-level facts and assumptions on which the Profile will be based to define its **scope**. An organization can have as many Organizational Profiles as desired, each with a different scope.

2 Gather the information

Examples of information may include organizational policies, risk management priorities and resources, enterprise risk profiles, business impact analysis (BIA) registers, cybersecurity requirementes…

3 Create the Organizational Profile

Determine **what types of information** the Profile should include for the selected CSF outcomes and document the needed information.

4 Analyze the gaps

Conduct **a gap analysis** to identify and analyze the differences between the Current and Target Profiles and develop a **prioritized action plan** to address those gaps.

5 Implement action plan

Follow the action plan to address the gaps and move the organization toward the Target Profile.

2 CSF Main Components

Tiers

Tiers characterize the rigor of an organization's cybersecurity risk governance and management practices, and provide context for how an organization views cybersecurity risks and the processes in place to manage those risks

	Cybersecurity Risk Governance	*Cybersecurity Risk Management*
Tier 1: Partial	• Application of **cybersecurity risk strategy** managed in **ad hoc manner**. • **Prioritization is ad hoc** and not formally based on objectives or threat environment.	• Implementation on an **irregular**, case-by-case basis. • There may not be processes that enable cybersecurity information to be shared within the organization. • **Unawareness of the cybersecurity risks associated** with suppliers and the products and services acquired and used.
Tier 2: Risk informed	• Practices are approved by management but may **not be established** as **organization-wide policy**. • The **prioritization of cybersecurity activities** and protection needs is **directly informed by organizational risk objectives**, the threat environment, or business/mission requirements.	• Awareness of cybersecurity risks but lack of comprehensive approach to managing them. • **Not consistently integrated across all levels**. Lack of repeatability or regularity in cyber risk assessments. Information sharing within the organization is informal. Lack of formal responses to cybersecurity risks associated with suppliers and products.
Tier 3: Repeatable	• Practices are **formally approved** and expressed as policy. • **Risk-informed policies**, processes, and procedures **are defined**, implemented as intended, and reviewed. • **Practices** are **regularly updated** based on the application of risk management processes to changes in business/mission requirements, threats, and technological landscape.	• **Cybersecurity information** is shared throughout the **organization-wide**. • **Consistent methods** in place **to respond effectively to risk changes**. Personnel with knowledge and skills to perform their roles and responsibilities. • **Consistently monitoring of cybersecurity risks of assets**. Senior executives communicate regularly cybersecurity risks, ensuring that cybersecurity is considered through all lines of operation in the organization.
Tier 4: Adaptative	• **Organization-wide approach** to managing cybersecurity risks. • **Cybersecurity risks and organizational objectives relation** clearly understood and considered when making decisions. • Business units implement the executive vision and analyze system-level risks in the context of risk tolerances. • Cybersecurity risk management is part of the **organizational culture.**	• **Adaptation** to a changing technological landscape and effectively respond to evolving sophisticated threats. • Use of **real-time information** to understand and consistently act upon the risks associated with its suppliers and the products and services it acquires and uses. Cybersecurity information is constantly shared throughout the organization and with authorized third parties.

3 Online Resources that Supplement the CSF

Informative References, Implementation Examples and Quick Start Guides

NIST and other organizations have produced a suite of online resources that help organizations understand, adopt, and use the CSF

Informative References	• Mappings that indicate relationships between the Core and various standards, guidelines, regulations, and other content. Informative References help inform how an organization may achieve the Core’s outcomes. • Informative References can be sector- or technology-specific. • They may be produced by NIST or another organization. Some Informative References are narrower in scope than a Subcategory. For example, Security and Privacy Controls for Information Systems and Organizations, may be one of many references needed to achieve the outcome described in one Subcategory. Other Informative References may be higher-level, such as a requirement from a policy that partially addresses numerous Subcategories. When using the CSF, an organization can identify the most relevant Informative References.
Implementation Examples	• They provide notional examples of concise, action-oriented steps to help achieve the outcomes of the Subcategories. Verbs used to express Examples include share, document, develop, perform, monitor, analyze, assess, and exercise. • The Examples are not a comprehensive list of all actions that could be taken by an organization to achieve an outcome, nor do they represent a baseline of required actions to address cybersecurity risks
QSGs	• Brief documents on specific CSF-related topics and are often tailored to specific audiences. QSGs can help an organization implement the CSF because they distill specific portions of the CSF into actionable first steps that an organization can consider on the path to improving their cybersecurity posture and management of associated risks. The guides are revised in their own time frames, and new guides are added as needed.

4 Improving Cybersecurity Risk Communication and Integration

Different CSF 2.0 uses

The CSF 2.0 also provides some insights about how it can be integrated into cybersecurity risk management

Improving Risk Management Communication	• The CSF facilitates **improved communication** regarding cybersecurity expectations, planning, and resource allocation within organizations. • It enables bi**directional information flow between executives, managers, and practitioners,** ensuring alignment with organizational priorities and strategic direction. • Through the **govern** function, executives engage in discussions about strategy and risk management, setting cybersecurity objectives and integrating them into enterprise risk management (ERM) programs. **Managers** focus on achieving risk targets through common services and controls, as outlined in the Target Profile, while **practitioners** implement these targets and measure changes in operational risk. As controls are implemented, practitioners provide relevant information to managers and executives to understand the organization's cybersecurity posture and make informed decisions. • **Executives** can also combine this cybersecurity risk data with information about other types of risk from across the organization. Updates to expectations and priorities are incorporated into updated Organizational Profiles as part of the continuous improvement cycle.
Improving Integration with other Risk Management Programs	• Every organization encounters various types of ICT risks. Some organizations integrate ICT risk management with other risk management efforts using ERM, while others keep these efforts separate. The NIST CSF helps translate cybersecurity terminology into general risk management language for executives. The CSF can be integrated with established cybersecurity risk management and several assessment programs. • **Privacy risks** intersect with cybersecurity. Cybersecurity management addresses privacy risks related to data confidentiality, integrity, and availability. Privacy risks can also arise independently from data processing activities, ranging from dignity-related effects to tangible harms. • Given the complex and interconnected relationships in this ecosystem, **supply chain risk management (SCRM)** is critical for organizations. Cybersecurity SCRM (C-SCRM) is a systematic process for managing exposure to cybersecurity risk throughout supply chains and developing appropriate response strategies, policies, processes, and procedures. • As **new technologies and new applications of technology** become available, new risks become clear. The NIST Artificial Intelligence Risk Management Framework (AI RMF) was developed to help address these risks. Treating AI risks alongside other enterprise risks.

5 Why Management Solutions?

In this regard, Management Solutions has a multi-sectoral and in-depth knowledge of key stakeholders, as well as strong capabilities to achieve practical results in a timely manner...

Proven experience in IT Risk and related projects

- **Trusted advisor in the implementation of risk and control models** *(Info&Data Sec., Physical Sec., Third Party, Technology, Data Mgmnt., Processes, Finance, People…).*
- **Methodology and framework analysis** *(COBIT, ICT, NIST, ITIL, SANS…)* Improvements paths identification and control frameworks definition.
- **Extensive experience in regulatory compliance projects, evolution and evaluation of compliance models.**
- **Supporting organizations in their review of processes, stakeholders, systems, etc. where the main sources of risk are located.**
- **In-depth knowledge of IT areas, technology platform (legacy and next gen) and active projects** in the main fields of action.

High-value profiles, expertise and cross vision

- Professionals with strong **understanding, communication, challenge/advice skills, expertise in Technology Risks and Cybersecurity, and their relationship with risk and process management (cross vision)**
- Understanding **of business processes, knowledge of risk management** methodologies and **analytical capabilities**
- **Detailed knowledge of regulations and best practices in market**

Experts in the development of functions for the management of IT risks

- **Comprehensive IT risk management programs and implementation of management frameworks and organizational models,** considering the evolution of the function and its pillars.
- **Definition and implementation of risk methodologies** with a defined risk appetite, risk assessment, valuation methodology and scenarios.
- **Definition of measurement objectives for the definition of IT risk management indicators and dashboards as a risk monitoring and reporting tool.**
- **Definition of IT and cybersecurity risk management indicators, risk appetite frameworks and quantification scenarios.**

Flagship firm with global capabilities

- **Global firm, independent and international** (+50 countries), with in-depth knowledge of the businesses in which our clients operate (+1800 global and local), selecting the most appropriate resources for each project, regardless of where they are located.
- **Multidisciplinary team** with strong analytical capabilities and specialist knowledge. Organized on a matrix basis (customer, industry, competitor and geography). Consultant accredited by **supervisors and supranational bodies** *(ECB, FCA, PRA, EIOPA, MEDE/ESM, WB…).*
- **Strong corporate culture:** commitment, dedication to service and constant pursuit of excellence.
- **Proven track record:** proven delivery capacity, which has been substantiated by significant organic growth (x42 in 21 years).
- **Benchmarking** capability (presence with Top IT customers in all geographies).

Access to regulatory and supervisory criteria

- **Experience with supervisory bodies.** We have large experience supporting European and American Supervisors in the supervision process.
- **Office in Frankfurt as Hub for regulatory analysis and liaison with the regulator** for regulatory issues, queries and anticipating requirements.

Management Solutions
Making things happen

International *One Firm*

Multiscope Team

Best practice *know-how*

Proven Experience

Maximum Commitment

Alejandro Iglesias Rodríguez
Partner at Management Solutions
alejandro.iglesias@msspain.com

Marta Hierro
Partner at Management Solutions
marta.hierro@msspain.com

The information contained in this publication is merely to be used as a guideline, is provided for general information purposes and is not intended to be used in lieu of consulting with our professionals. Management Solutions is not liable for any use that third parties may make of this information. The use of this material is not permitted without the express authorization of Management Solutions.

For more information please visit

www.managementsolutions.com

Or follow us at: