SECURITY AND RISK: MANAGEMENT AND CERTIFICATIONS

Simone **Soderi**

M1.2 - Basic Concepts

Contents

1. **Cybersecurity fundamentals**
   - Definitions and basics concepts
   - Knowledge areas
   - Why are risk assessment and management important?
2. **Standards overview**
   - Standard of Good Practice
   - ISO/IEC 27000 Suite
   - ISA/IEC 62443
3. **Frameworks overview**
   - NIST Cybersecurity Framework
   - MITRE Att&ck
   - National Framework for Cybersecurity
   - OWASP
4. **Effective Cybersecurity**
   - Management process
   - Cybersecurity information and decision flow

Contents

NIST

US OFFICE OF COMMERCE

NIST is a U.S. federal agency that deals with measurement science, standards, and technology related to the U.S. government and to the promotion of U.S. private sector innovation.

- Despite their national scope, NIST Federal Information Processing Standards (FIPS) and **Special Publications (SP) have a worldwide impact**.
- In the area of information security, the **NIST Computer Security Resource Center (CSRC)** is the source of a vast collection of documents that are widely used in the industry.

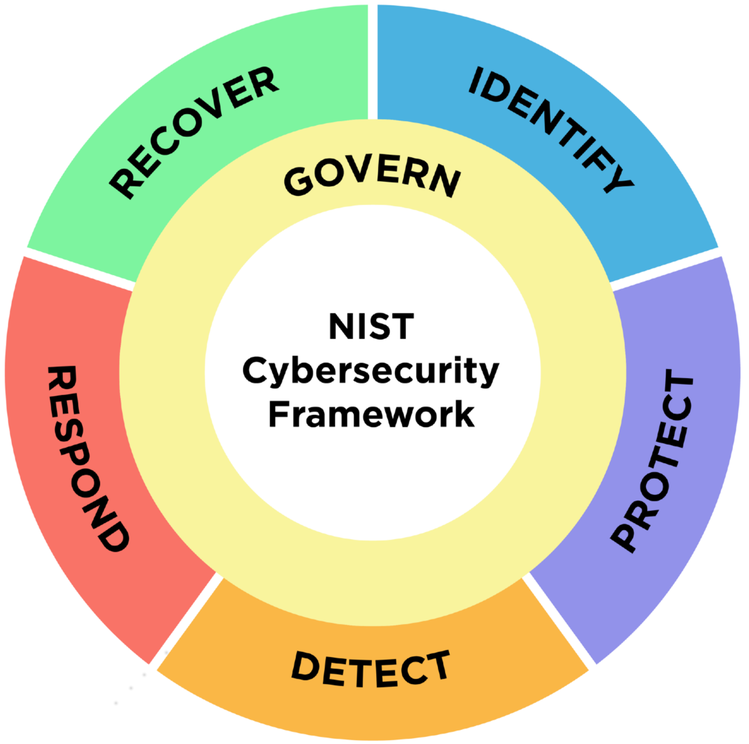
  https://csrc.nist.gov/

NIST Cybersecurity Framework (1/3)

NIST CSF

In response to the **growing number of cyber intrusions** at U.S. federal agencies, Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, directed the **NIST to work with stakeholders** to develop a **voluntary framework for reducing cyber risks to critical infrastructure.**

The framework is a collection of best practices that improve efficiency and protect components. Although provided for federal agencies, **the document is of use for nongovernment organizations**.



NIST Cybersecurity Framework (CSF) 2.0 issued February 26, 2024

NIST Cybersecurity Framework (2/3)

NIST CSF

CORE

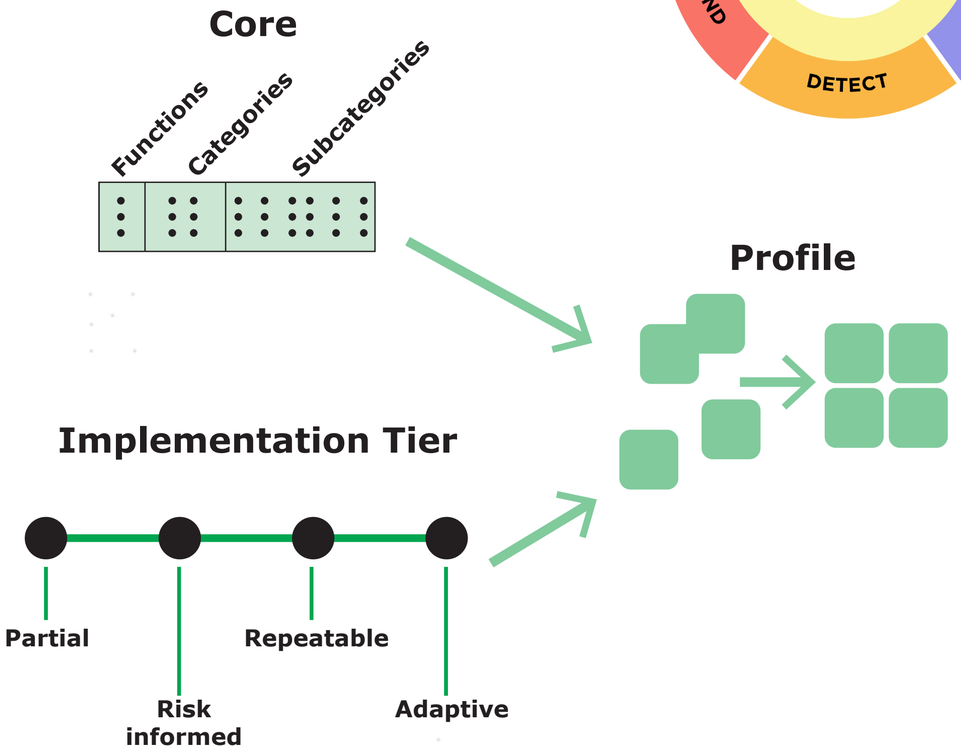
Provides a set of cybersecurity **activities**, desired **outcomes**, and applicable **references** that are common across critical infrastructure sectors

IMPLEMENTATION TIERS

Provide **context** on how an organization views cybersecurity risk and the processes in place to manage that risk

PROFILES

Represents the outcomes based on **business needs** that an organization has selected from the Framework Core **categories** and **subcategories**



CSF Components

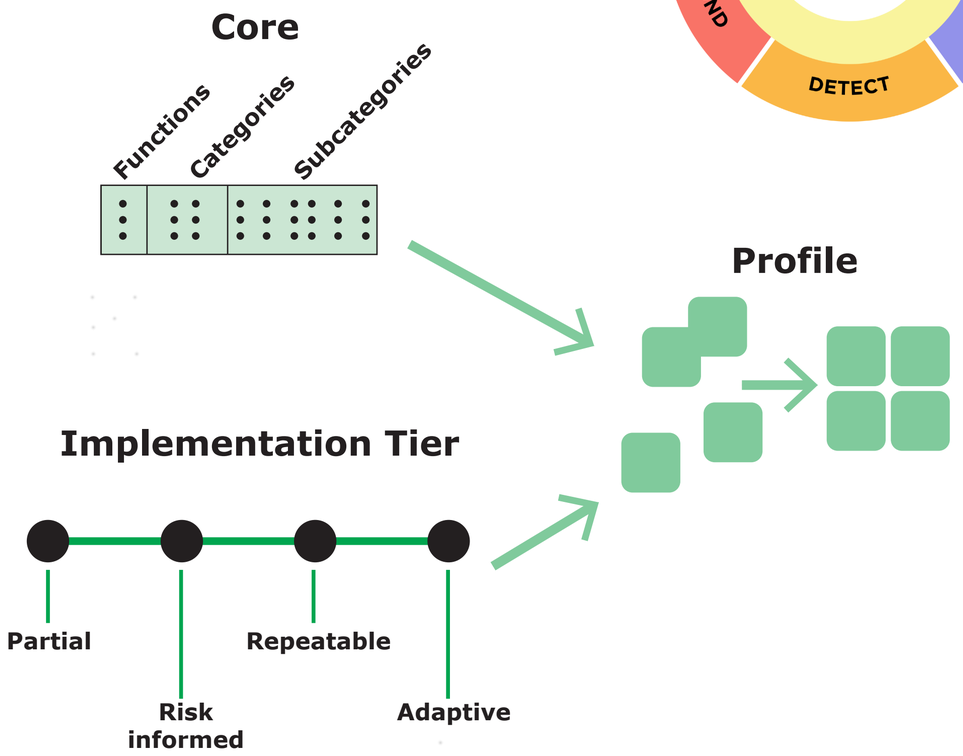
https://www.nist.gov/cyberframework

NIST Cybersecurity Framework (3/3)

NIST CSF

AN ORGANIZATION CAN USE THE CSF CORE, PROFILES, AND TIERS WITH THE SUPPLEMENTARY RESOURCES TO UNDERSTAND, ASSESS, PRIORITIZE, AND COMMUNICATE CYBERSECURITY RISKS.

- **Understand and Assess**: Describe the current or target cybersecurity posture of part or all of an organization, determine gaps, and assess progress toward addressing those gaps.
- **Prioritize:** Identify, organize, and prioritize actions for managing cybersecurity risks that align with the organization's mission, legal and regulatory requirements, and risk management and governance expectations.
- **Communicate:** Provide a common language for communicating inside and outside theorganization about cybersecurity risks, capabilities, needs, and expectations



CSF Components

NIST CSF Core Functions

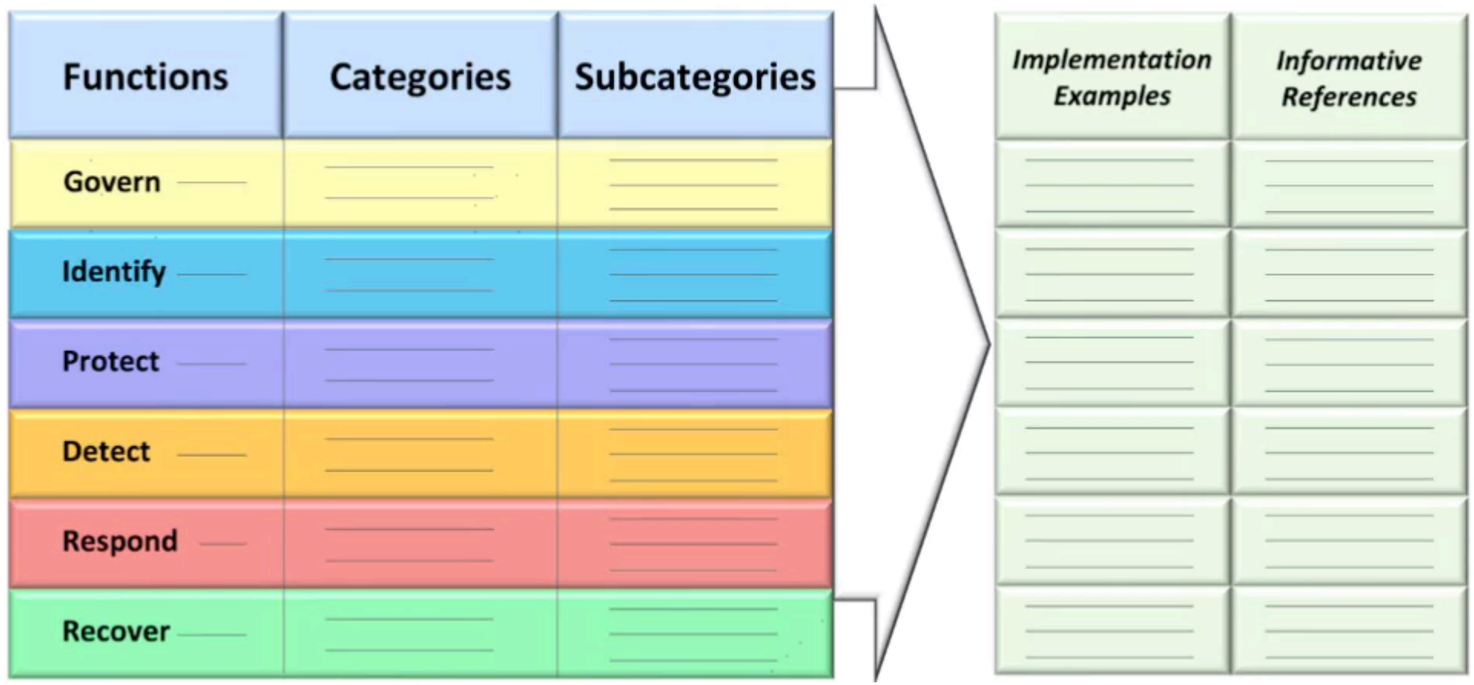
CORE COMPONENT

The Framework Core identifies **six key functions** that compose an organization's cybersecurity risk management approach. Each function is divided into a number of specific **categories**, each of which in turn is divided into a number of more detailed subcategories,

The six functions **provide a high-level view of the elements** that compose risk management for an organization.

Each category is divided into **subcategories** of specific outcomes of technical and/or management activities that provide

For each subcategory the NIST Cybersecurity Framework **provides a list of informative references**, **which are specific sections of standards, guidelines, and practices common among critical infrastructure sectors** that illustrate methods of achieving the outcomes associated with each subcategory.



NIST Cybersecurity Framework (CSF) 2.0 Reference Tool allows users to explore the CSF 2.0 Core

NIST CSF Implementation Tiers

LEVEL OF COMMITMENT

The **tiers** defined in the Cybersecurity Framework help an organization **define the priority** that is to be given to cybersecurity and the **level of commitment** that the organization intends to make.

The tiers range from **Partial (Tier 1)** to **Adaptive (Tier 4)** and **describe increasing degrees of rigor and sophistication in cybersecurity risk management practices** and the **extent** to which cybersecurity risk management is informed by business needs and **integrated** into an organization's overall risk management practices

Risk Management Process	Integrated Risk Management Program	External Participation
Tier 1: Partial		
RM practices not formalized, ad hoc. Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements.	Limited awareness of risk, no organization-wide approach to RM. cybersecurity information to be shared within the organization.	Lack of coordination and collaboration with other entities.
Tier 2: Risk Informed		
RM practices approved by management by not established as organizational-wide policy. Informed prioritization of cybersecurity activities.	Risk-informed, processes and procedures are defined and implemented, and staff has adequate resources to perform their cybersecurity duties. No organization-wide approach to RM.	No formal coordination and collaboration with other entities.
Tier 3: Repeatable		
RM practices are formally approved and expressed as policy. Organizational cybersecurity practices are regularly updated based on changes in business/mission requirements and the threat and technology landscape.	Organization-wide approach to RM. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities.	Collaboration with partners enables RM decisions in response to external events.
Tier 4: Adaptive		
Organization actively adapts to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner.	Organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events.	Organization manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed.

NIST CSF Small Business Using Tiers

Check for updates

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Cybersecurity Framework 2.0: Quick-Start Guide for Using the CSF Tiers

U.S. Department of Commerce
Gina M. Raimondo, Secretary
National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

NIST Special Publication
NIST SP 1302 ipd (Initial Public Draft)
The public comment period for this draft ends May 3, 2024.
Please send your comments to cyberframework@nist.gov.
https://doi.org/10.6028/NIST.SP.1302.ipd
February 2024

NIST CSF Profiles

STEPS FOR CREATING PROFILES

- A **profile** is a selection of categories and subcategories from the Framework Core.
- A **current profile** reflects the **cybersecurity posture of the organization**. Based on a risk assessment, an organization can define a **target profile** and then categories and subcategories from the Framework Core to reach the target. This definition of current and target profiles **enables management** to determine what has been done and **needs to be maintained and what new cybersecurity measures** need to be implemented to manage risk.
- The referenced **guidelines**, standards, and practices for each subcategory provide **concrete descriptions** of the work needed to meet the target profile.

NIST CSF Small Business Quick-Start Guide

Check for updates

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

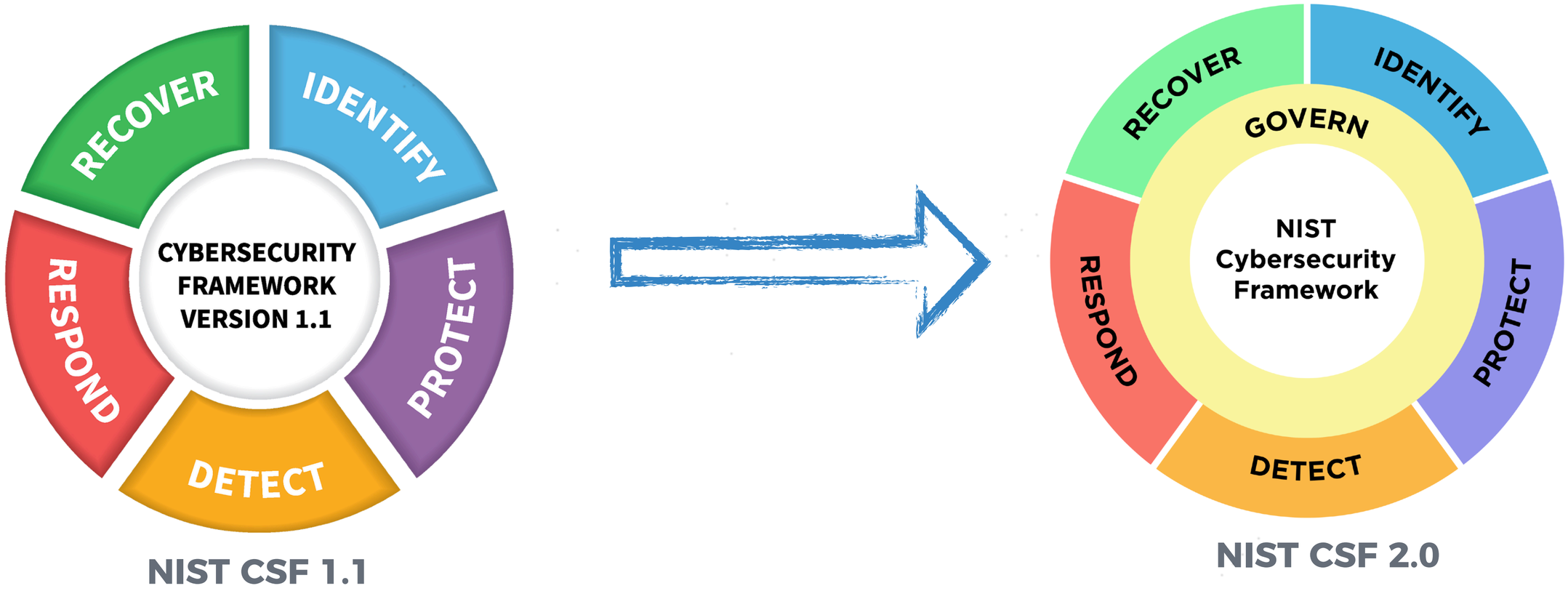
NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide

U.S. Department of Commerce
Gina M. Raimondo, Secretary
National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

NIST Special Publication
NIST SP 1300
https://doi.org/10.6028/NIST.SP.1300
February 2024

NIST CSF 2.0: a significant revision

CSF 1.1. VS CSF 2.0



1. The CSF 2.0 introduces a **new function called "Govern,"** which emphasises the significance of organisational governance in cybersecurity.
2. The CSF 2.0 emphasizes the importance of **managing supply chain risk**, which is a growing concern for organizations.
3. The CSF 2.0 encourages organizations to **adopt a mindset of continuous improvement**, rather than a one-time assessment and implementation.

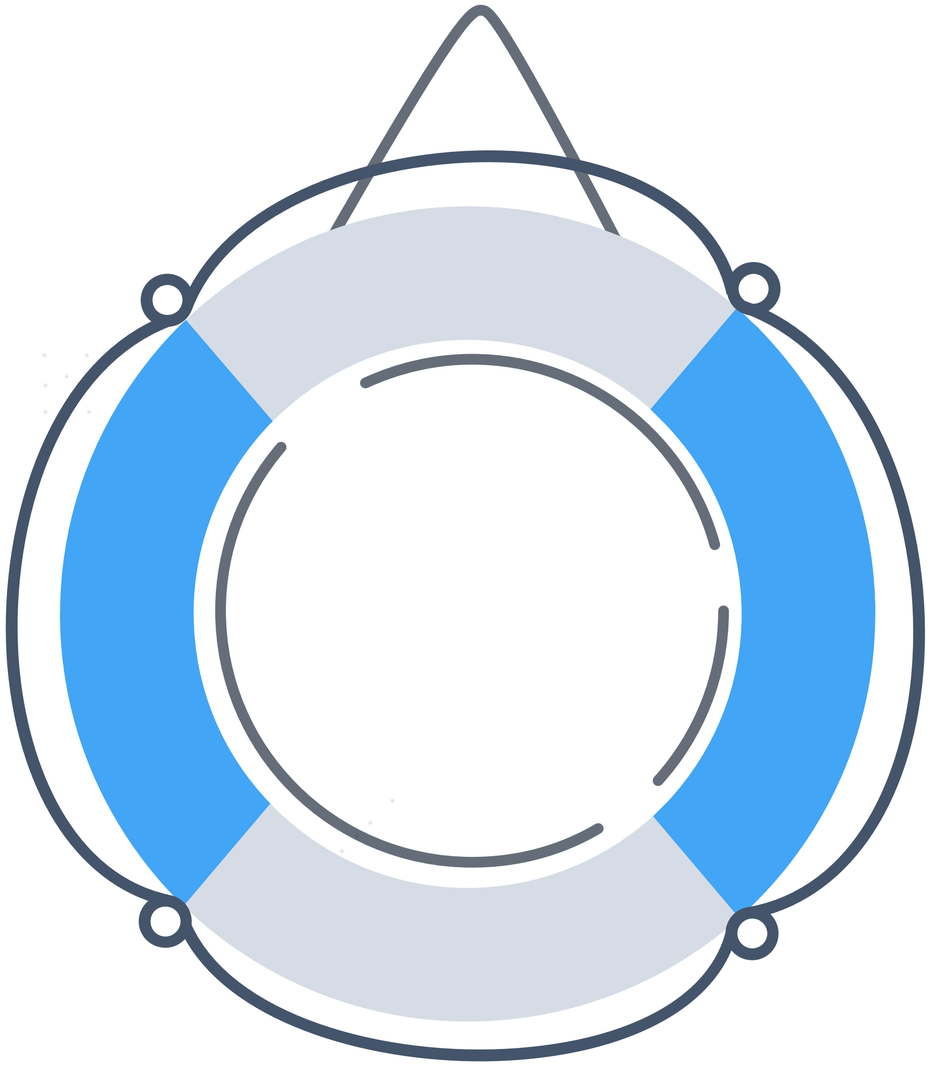
NIST CSF

GENERAL COMMENT

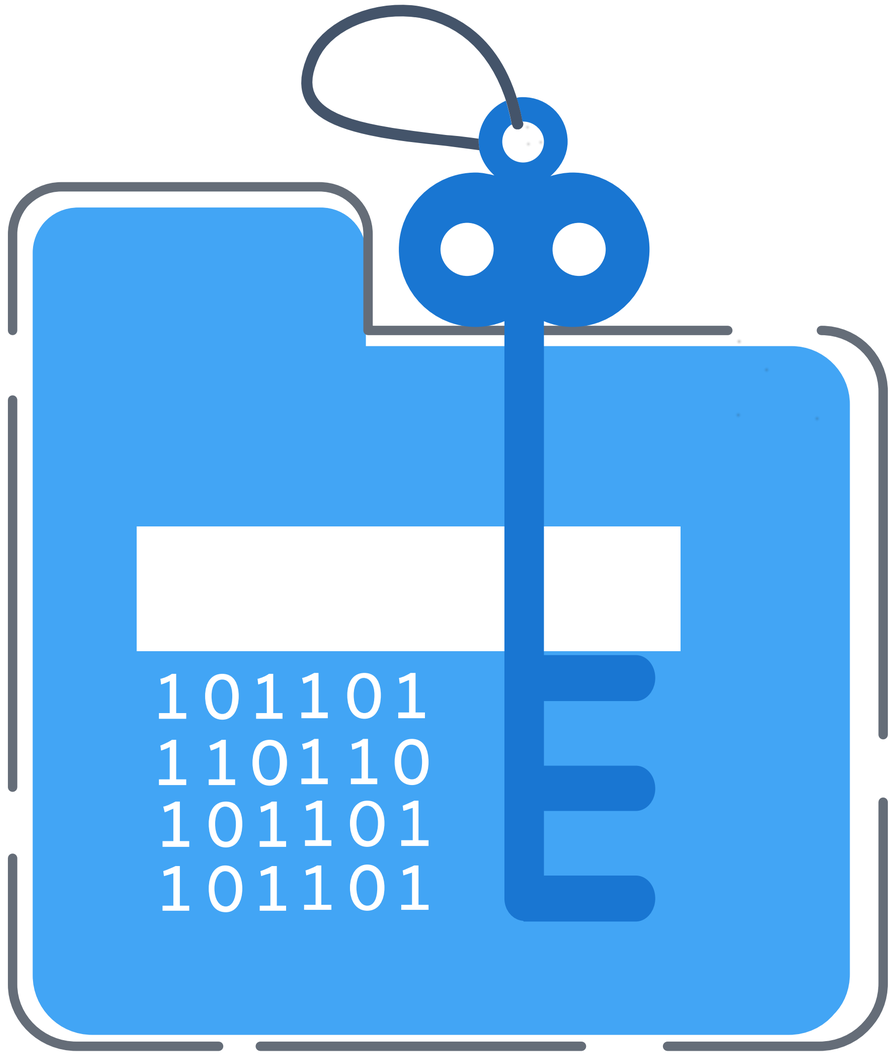
The **NIST Cybersecurity Framework** is an **important resource** for those involved in the planning, implementation, and evaluation of an organization's cybersecurity capability.

It is concise and uses clearly defined categories and subcategories. Approaching a document such as the ISF SGP or the ISO 27002 can be **intimidating** and even overwhelming because of the large body of knowledge they contain.

The Cybersecurity Framework is an **excellent resource** to help an organization more effectively use these more detailed **documents**.



NIST Security Documents: what?



NIST has produced a large number of FIPS publications and SPs that are enormously useful to security managers, designers, and implementers. Some of these documents are **prescriptive standards**, but many of them are **tutorials or surveys** and provide a continually updated source of educational material on a broad range of security topics.

Special Publications (SPs).

Federal Information Processing Standards (FIPS)

Countermeasures

Technical Safeguards

An action, a device, a procedure, or a technique **that reduces a threat, a vulnerability, or an attack** by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

NIST Security Documents: most important ones

NIST SP 800-53, ***Security and Privacy Controls for Federal Information Systems and Organizations***

This document lists management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. **State-of-the-practice security controls and control enhancements** have been integrated into the latest revision (2013) to address the evolving technology and threat space.

FIPS 200, Minimum Security Requirements for Federal Information and Information Systems (2006)

Specifies minimum security requirements in 17 security-related areas with regard to protecting the confidentiality, integrity, and availability of federal information systems and the information processed, stored, and transmitted by those systems.

NIST SP 800-12, Introduction to Information Security, (2017)

Provides an outstanding **introduction to the topic of information security.**

NIST SP 800-55, Performance Measurement Guide for Information Security (2008)

Provides guidance on how an organization, through the use of metrics, identifies the adequacy of in-place security controls, policies, and procedures.

SP 800-100, Information Security Handbook: A Guide for Managers (2006)

Provides a broad overview of **information security program elements to assist managers in understanding how to establish and implement an information security program**. Its topical coverage overlaps considerably with ISO 27002.

MITRE

"AT MITRE, WE SOLVE PROBLEMS FOR A SAFER WORLD"

The **MITRE Corporation** was chartered in 1958 as a private, not-for-profit company to provide engineering and **technical guidance for the federal government**.

MITRE **works in the public interest** across federal, state and local governments, as well as industry and academia. We bring innovative ideas into existence in areas as varied as artificial intelligence, intuitive data science, quantum information science, health informatics, space security, policy and economic expertise, trustworthy autonomy, cyber threat sharing, and cyber resilience.

MITRE supports various U.S. government agencies in the aviation, defense, healthcare, homeland security, and **cybersecurity fields**, among others.

https://www.mitre.org/

MITRE Att&ck: Why?

THE MOTIVATIONS BEHIND ITS DEVELOPMENT

MITRE started ATT&CK in 2013

to document common **tactics**, **techniques**, and **procedures** (**TTPs**) that advanced persistent threats use against Windows enterprise networks. This framework to address **four main issues**:

- **Adversary behaviours.** Focusing on adversary **tactics** and techniques allowed us to develop analytics to detect possible adversary behaviours. Typical indicators such as domains, IP addresses, file hashes, registry keys, etc. were easily changed by adversaries and were only useful for point in time detection — they didn't represent how adversaries interact with systems, only that they likely interacted at some time.
- **Lifecycle models that didn't fit.** Existing adversary lifecycle and **Cyber Kill Chain concepts** were too high-level to relate behaviours to defenses — the level of abstraction wasn't useful to map TTPs to new types of sensors.
- **Applicability to real environments.** TTPs need to be based on **observed incidents** to show the work is applicable to real environments.
- **Common taxonomy.** TTPs need to be comparable across different types of adversary groups using the same terminology.

MITRE Att&ck Framework

KNOWLEDGE BASE DOCUMENTS

MITRE ATT&CK is an open framework for implementing cybersecurity detection and response programs.

The ATT&CK framework is available **free of charge** and includes a global knowledge base of adversarial **tactics, techniques, and procedures (TTPs)** based on real-world observations. **ATT&CK mimics** the behaviour of real-life attackers, **helping** IT, security, and compliance organizations **efficiently identify** security gaps, evaluate risks, and eliminate vulnerabilities.

Common taxonomy

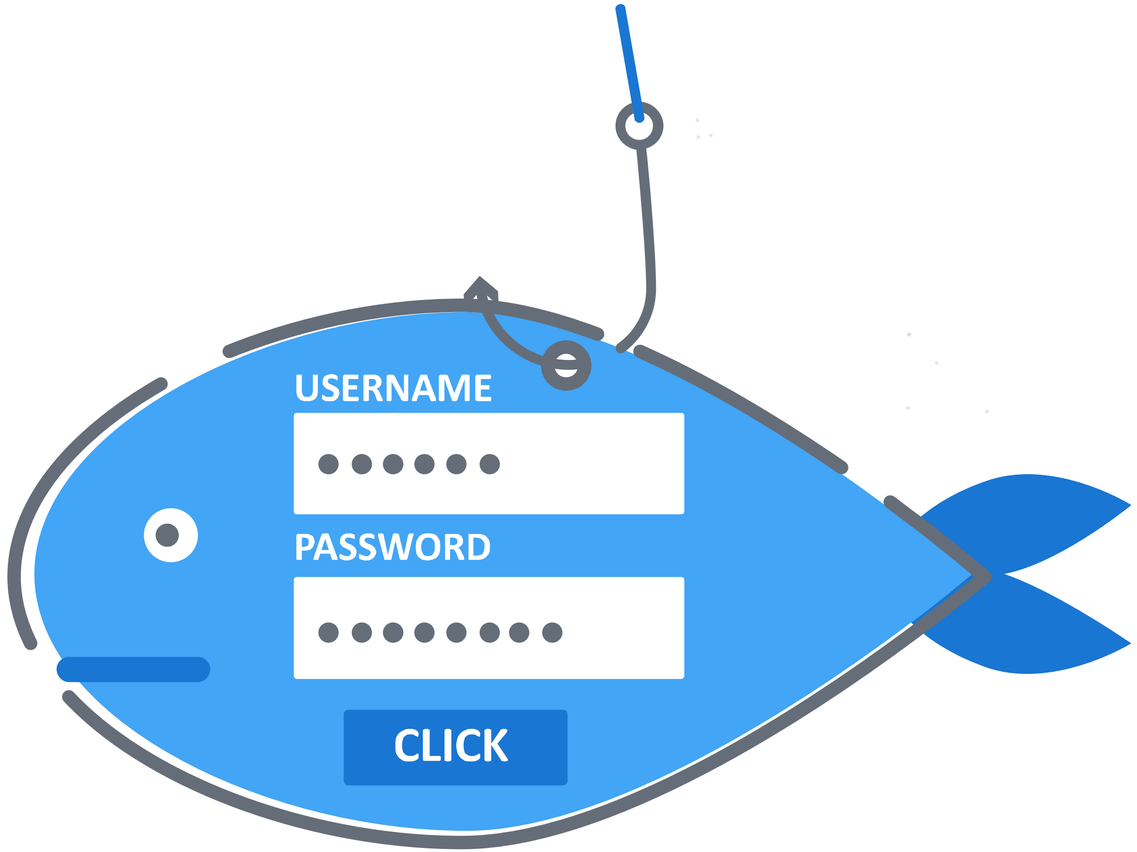
ATT&CK provides a **common taxonomy** that lets various constituents (SecOps teams, red and blue teams, penetration testers, security solution providers, threat intelligence vendors, etc.) communicate using the **same language**.

Database

ATT&CK also includes a **Groups database** that **tracks the activities** of threat actors and cybercriminal syndicates around the world.

MITRE Att&ck TTPs

TACTICS VS TECHNIQUES



ATT&CK is largely a knowledge base of adversarial techniques

Unlike prior work in this area, the focus isn't on the tools and **malware that adversaries use but on how they interact** with systems during an operation. ATT&CK organizes these techniques into a set of tactics to help explain to provide context for the technique.

TATICS

Tactics represent the **"why"** of an ATT&CK technique. The tactic is the adversary's tactical objective for performing an action

TECHNIQUES

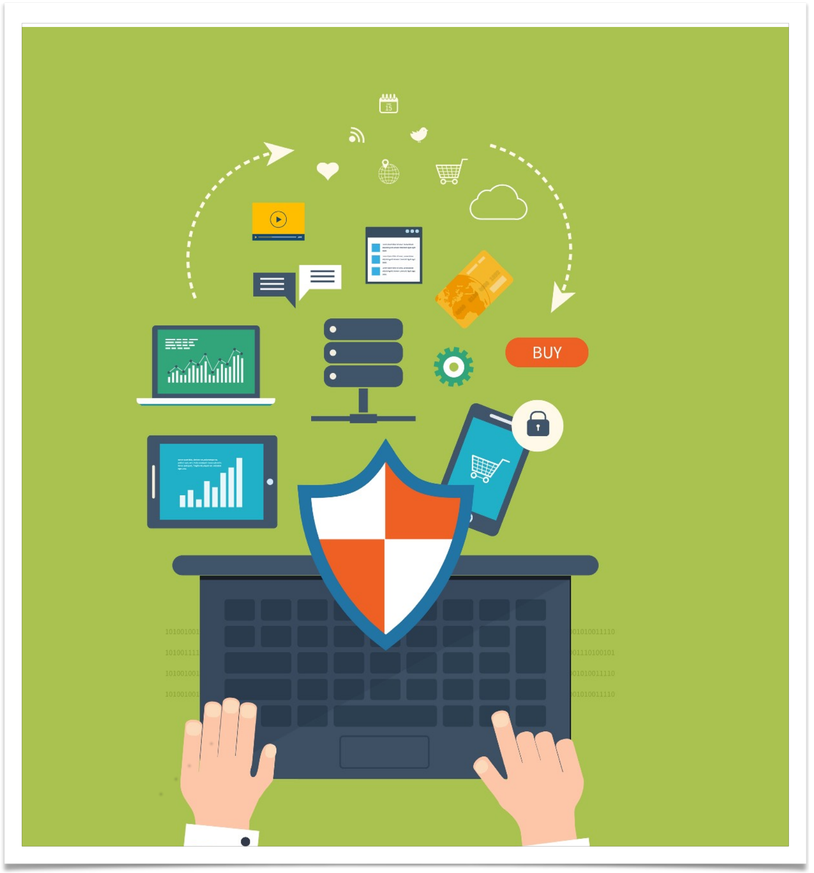
Techniques represent **"how"** an adversary achieves a tactical objective by performing an action. Techniques may also represent **"what"** an adversary gains by performing an action.

MITRE Att&ck Background and Scope

KNOWLEDGE BASE DOCUMENTS

Since 2013, MITRE has identified hundreds of different techniques adversaries use to execute cyberattacks. **ATT&CK organizes these techniques into a collection of tactics to help security practitioners efficiently detect, isolate, and remediate threats.**

The **tactics** describe what the **adversary is trying to do** (e.g., steal credentials) and the **techniques** describe **the actions the adversary takes** to achieve their goals (e.g., brute force methods).



ATT&CK FOR ENTERPRISE MATRIX

for Windows, macOS, Linux, cloud, containers, and network systems

https://attack.mitre.org/versions/v12/

ATT&CK FOR MOBILE MATRIX

for Apple iOS and Android devices

https://attack.mitre.org/matrices/mobile/

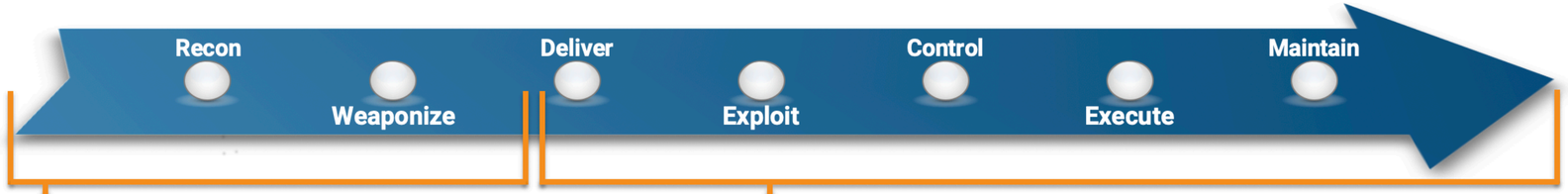
ATT&CK FOR INDUSTRIAL CONTROL SYSTEMS MATRIX

for Supervisory Control and Data Acquisition (SCADA) systems and other industrial control systems

https://collaborate.mitre.org/attackics/index.php/Main_Page

MITRE Att&ck Decomposition

PROCESS FOR ENTERPRISE



PRE-ATT&CK

Priority Definition
- **Planning, Direction**

Target Selection
Information Gathering
- **Technical, People, Organizational**

Weakness Identification
- **Technical, People, Organizational**

Adversary OpSec
Establish & Maintain Infrastructure
Persona Development
Build Capabilities
Test Capabilities
Stage Capabilities

ATT&CK for Enterprise

Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
Command and Control
Impact

All steps needed to execute a cyber-attack can be divided over **these seven stages.**

The first two stages are broadly covered by Mitre's PRE-ATT&CK, and the other five by the ATT&CK framework.

PRE-ATT&CK

the PRE-ATT&CK framework focusses on **the preceding preparation phases.** Preventing an attack is **much cheaper** than having to repair damages to IT systems, let alone the financial or reputational impact it can have.

ATT&CK FOR ENTERPRISE

ATT&CK framework concentrates on the steps taken once an attack is launched

MITRE Att&ck Matrix

ENTERPRISE

Reconnaissance 10 techniques	Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 14 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (0/2)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation (0/4)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Brute Force (0/4)	Account Discovery (0/4)	Exploitation of Remote Services	Archive Collected Data (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Credentials from Password Stores (0/3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/6)	External Remote Services	Inter-Process Communication (0/2)	Boot or Logon Autostart Execution (0/12)	Boot or Logon Autostart Execution (0/12)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (0/2)	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Clipboard Data	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Scheduled Task/Job (0/6)	Browser Extensions	Create or Modify System Process (0/4)	Direct Volume Access	Input Capture (0/4)	Cloud Service Dashboard	Remote Services (0/6)	Data from Cloud Storage Object	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution (0/15)	Execution Guardrails (0/1)	Man-in-the-Middle (0/2)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (0/2)	Encrypted Channel (0/2)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Search Closed Sources (0/2)		Supply Chain Compromise (0/3)	Software Deployment Tools	Create Account (0/3)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Modify Authentication Process (0/4)	Domain Trust Discovery	Software Deployment Tools	Data from Information Repositories (0/2)	Fallback Channels	Exfiltration Over Web Service (0/2)	Endpoint Denial of Service (0/4)
Search Open Technical Databases (0/5)		Trusted Relationship	System Services (0/2)	Create or Modify System Process (0/4)	Group Policy Modification	File and Directory Permissions Modification (0/2)	Network Sniffing	File and Directory Discovery	Taint Shared Content	Data from Local System	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (0/2)		Valid Accounts (0/4)	User Execution (0/2)	Event Triggered Execution (0/15)	Hijack Execution Flow (0/11)	Group Policy Modification	OS Credential Dumping (0/8)	Network Service Scanning	Use Alternate Authentication Material (0/4)	Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			Windows Management Instrumentation	External Remote Services	Process Injection (0/11)	Hide Artifacts (0/7)	Steal Application Access Token	Network Share Discovery		Data from Removable Media	Non-Application Layer Protocol		Network Denial of Service (0/2)
				Hijack Execution Flow (0/11)	Scheduled Task/Job (0/6)	Hijack Execution Flow (0/11)	Steal or Forge Kerberos Tickets (0/4)	Network Sniffing		Data Staged (0/2)	Non-Standard Port		Resource Hijacking
				Implant Container Image	Valid Accounts (0/4)	Impair Defenses (0/7)	Steal Web Session Cookie	Password Policy Discovery		Email Collection (0/3)	Protocol Tunneling		Service Stop
				Office Application Startup (0/6)		Indicator Removal on Host (0/6)	Two-Factor Authentication Interception	Peripheral Device Discovery		Input Capture (0/4)	Proxy (0/4)		System Shutdown/Reboot
				Pre-OS Boot (0/5)		Indirect Command Execution	Unsecured Credentials (0/6)	Permission Groups Discovery (0/3)		Man in the Browser	Remote Access Software		
				Scheduled Task/Job (0/6)		Masquerading (0/6)		Process Discovery		Man-in-the-Middle (0/2)	Traffic Signaling (0/1)		
				Server Software Component (0/3)		Modify Authentication Process (0/4)		Query Registry		Screen Capture	Web Service (0/3)		
						Modify Cloud Compute Infrastructure (0/4)		Remote System Discovery		Video Capture			
								Software Discovery (0/1)					

MITRE Att&ck Matrix

Tactics: the adversary's technical goals

Techniques: how the goals are achieved

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	Scheduled Task			Binary Padding	Network Sniffing		AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	Launchctl		Access Token Manipulation		Account Manipulation	Account Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
	Local Job Scheduling		Bypass User Account Control		Bash History	Application Window Discovery		Clipboard Data		Data Encrypted	Defacement
External Remote Services	LSASS Driver		Extra Window Memory Injection		Brute Force		Distributed Component Object Model	Data from Information Repositories	Connection Proxy	Data Transfer Size Limits	Disk Content Wipe
Hardware Additions	Trap		Process Injection		Credential Dumping	Browser Bookmark Discovery			Custom Command and Control Protocol	Exfiltration Over Other Network Medium	Disk Structure Wipe
Replication Through Removable Media	AppleScript	DLL Search Order Hijacking			Credentials in Files		Exploitation of Remote Services	Data from Local System			Endpoint Denial of Service
	CMSTP	Image File Execution Options Injection			Credentials in Registry	Domain Trust Discovery		Data from Network Shared Drive	Custom Cryptographic Protocol	Exfiltration Over Command and Control Channel	Firmware Corruption
Spearphishing Attachment	Command-line Interface	Plist Modification			Exploitation for Credential Access	File and Directory Discovery	Logon Scripts				Inhibit System Recovery
Spearphishing Link	Compiled HTML File	Valid Accounts				Network Service Scanning	Pass the Hash	Data from Removable Media	Data Encoding	Exfiltration Over Alternative Protocol	Network Denial of Service
Spearphishing via Service	Control Panel Items	Accessibility Features		BITS Jobs	Forced Authentication	Network Share Discovery	Pass the Ticket	Data Staged	Data Obfuscation		Resource Hijacking
Supply Chain Compromise	Dynamic Data Exchange	AppCert DLLs		Clear Command History	Hooking	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Fronting	Exfiltration Over Physical Medium	Runtime Data Manipulation
Trusted Relationship	Execution through API	AppInit DLLs		CMSTP	Input Capture	Peripheral Device Discovery	Remote File Copy	Input Capture	Domain Generation Algorithms		Service Stop
Valid Accounts	Execution through Module Load	Application Shimming		Code Signing	Input Prompt	Permission Groups Discovery	Remote Services	Man in the Browser		Scheduled Transfer	Stored Data Manipulation
		Dylib Hijacking		Compiled HTML File	Kerberoasting	Process Discovery	Replication Through Removable Media	Screen Capture	Fallback Channels		Transmitted Data Manipulation
	Exploitation for Client Execution	File System Permissions Weakness		Component Firmware	Keychain	Query Registry		Video Capture	Multiband Communication		
		Hooking		Component Object Model Hijacking	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Shared Webroot		Multi-hop Proxy		
	Graphical User Interface	Launch Daemon				Security Software Discovery	SSH Hijacking		Multilayer Encryption		
	InstallUtil	New Service		Control Panel Items	Password Filter DLL	System Information Discovery	Taint Shared Content		Multi-Stage Channels		
	Mshta										
	PowerShell										
	Regsvcs/Regasm	Serv									
	Regsvr32										
	Rundll32										
	Scripting										
	Service Execution	.bash_profile a									
	Signed Binary Proxy Execution	Account Man									
		Authentication									
	Signed Script Proxy Execution	BITS J									
		Bootk									
	Source	Browser Ext									
	Space after Filename	Change D File Assoc									
	Third-party Software										
	Trusted Developer Utilities	Component F									
	User Execution	Component Model Hija									
	Windows Management Instrumentation	Create Ac									
	Windows Remote Management	External Remo									
		Hidden Files an									
	XSL Script Processing	Hypervisor									
		Kernel Modules and Extensions									
						from Tools					
						Indicator Removal on Host					
						Indirect Command Execution					

Procedures: Specific technique implementation

Spearphishing Attachment

Procedure Examples

Name	Description
APT12	APT12 has sent emails with malicious Microsoft Office documents and PDFs attached. [88] [89]
APT19	APT19 sent spearphishing emails with malicious attachments in RTF and XLSM formats to deliver initial exploits. [62]

https://mitre-attack.github.io/attack-navigator/

Cybersecurity in Italy

MAIN MILESTONES

2016 ITALIAN CYBERSECURITY REPORT

15 FUNDAMENTAL SECURITY **CONTROLS** FOR SMALL AND MICRO BUSINESSES

DPCM FEB. 17TH, 2016

IMPORTANT ACTION TO **IMPROVE** THE ITALIAN CYBERSECURITY **PROGRAM**

LIBRO BIANCO, JAN. 2018

"IL FUTURO DELLA CYBERSECURITY IN ITALIA: AMBITI PROGETTUALI STRATEGICI PROGETTI E AZIONI PER DIFENDERE AL MEGLIO IL PAESE DAGLI ATTACCHI INFORMATICI"

NIS DIRECTIVE IMPLEMENTATION, MAY 2018 (D.LGS. 65/2018)

ENSURING SECURITY OF NETWORKS AND INFORMATION SYSTEMS, WHICH APPLIES TO:
ESSENTIAL SERVICES OPERATORS (**OSE**) AND DIGITAL SERVICES PROVIDERS (**FSD**);
CREATION OF THE COMPUTER SECURITY INCIDENT RESPONSE TEAM (**CSIRT**)

NATIONAL FRAMEWORK FOR CYBERSECURITY AND DATA PROTECTION, FEB. 2019

IT UPDATES THE FIRST VERSION ISSUED IN 2015.

NATIONAL CYBERSECURITY PERIMETER, NOV. 2019 (L. 133/2019)

THE NEW LAW AIMS TO ENSURE THE SECURITY OF NETWORKS AND ITS SYSTEMS **BY PREVENTING** THEIR MALFUNCTIONING, INTERRUPTION, AND IMPROPER USE.

THE WELFARE OF ONE'S COUNTRY & DEGREE OF SECURITY OF ITS CYBERSPACE

NATO OFFICIALLY RECOGNISES THE CYBERSPACE AS THE FIFTH DOMAIN OF A WARFARE SO IT COULD RESPOND WITH CONVENTIONAL WEAPONS IN CASE OF A POWERFUL CYBER ATTACK.

National Framework for Cybersecurity (Italy)

ITALY USE CASE

The **National Framework for Cybersecurity and Data Protection ("Framework")** represents a **tool for measuring an organization's security posture in terms of maturity and completion of activities aimed at reducing cyber risk.**

Published in Italy in 2015 and updated in **2019 to version 2.0** in order to capture the Data Protection aspects expressed in the **GDPR**, the Framework allows for an in-depth look at several dimensions inherent to cybersecurity.

Designed to be used by public and private organizations of different sizes, the **Framework** is characterized by a series of key elements, which **take up and integrate** what has been proposed by **NIST with its Cybersecurity Framework**.

https://www.cybersecurityframework.it/

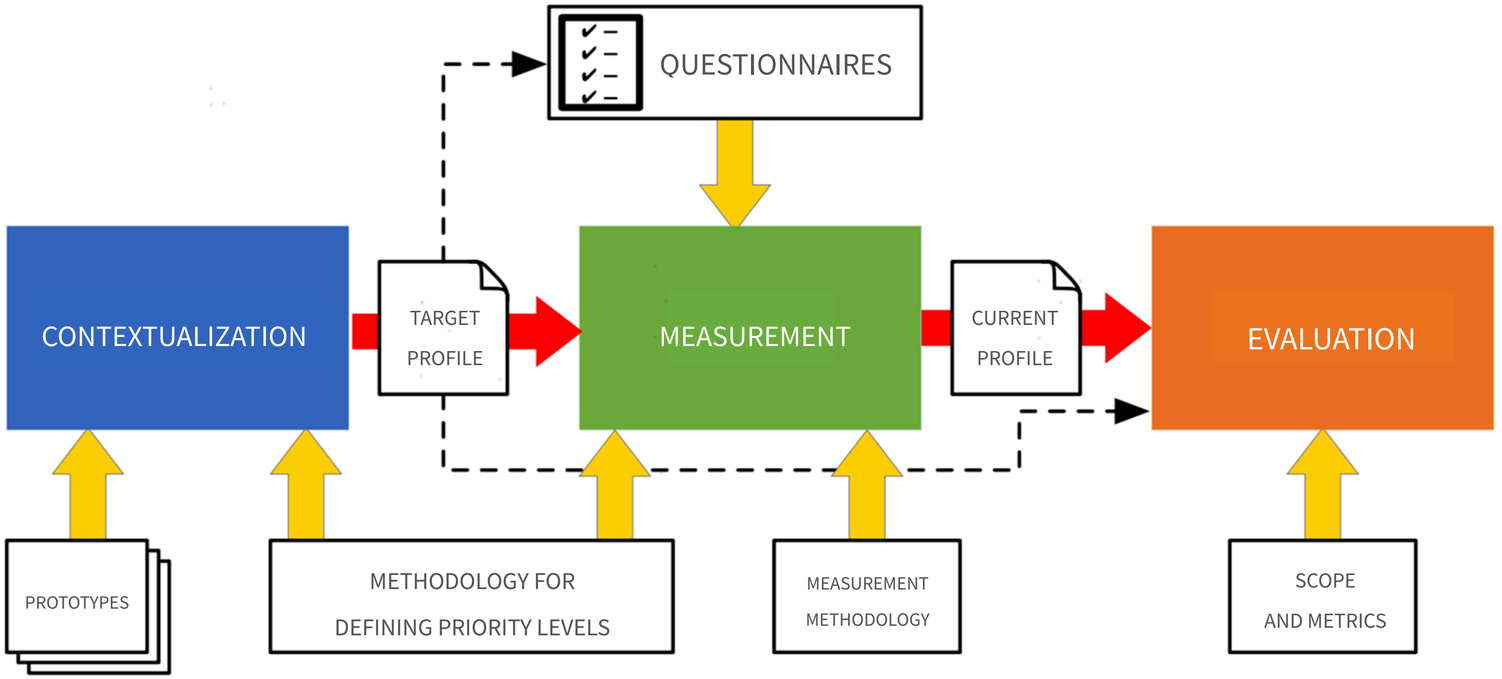
Framework Principles

KEY ELEMENTS

Principle	Description
CORE	Structured **list of requirements** needed to achieve different security objectives. The requirements are organized into Function (Identify, Protect, Detect, Respond, Recovery), Category and Subcategory.
CONTROLS	A **set of actions** into which the requirements expressed by the subcategories can be declined. They are to be defined according to the characteristics and needs of each organization.
INFORMATIVE REFERENCES	References that **tie each subcategory to known security practices** provided for in current general regulations (e.g., GDPR, NIS, etc.) and industry standards (e.g., ISO, COBIT-5, SANS20, etc.).
PRIORITIES LEVELS	Levels (High, Medium, Low) **indicating the priority of implementation** of the requirements indicated in each subcategory.
MATURITY LEVELS	**Implementation** maturity levels of subcategories and controls.
CONTEXTUALIZATION	**Process of selecting subcategories** of interest to the organization and assessing priority and maturity levels for the selected subcategories.
PROTOTYPE OF CONTEXTUALIZATION	Support **templates to implement contextualization**, based on guidance provided by information references, industry best practices and internal security policies within the organization.

Framework Methodology (1/3)

THREE PHASES



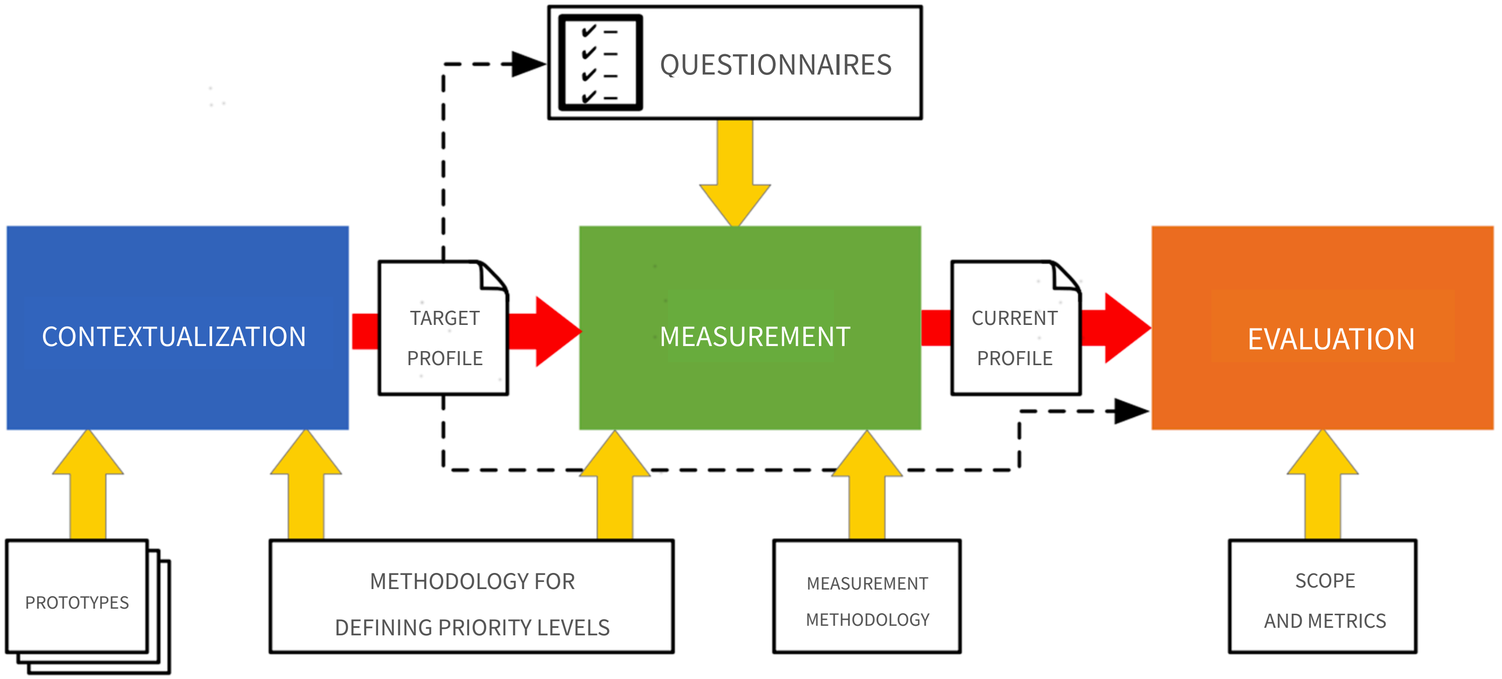
PHASE 1 - CONTEXTUALIZATION

This first phase aims at **contextualizing the Framework to the reality of interest**. This phase, as detailed in, can make use of specific support tools called contextualization prototypes, already published or defined ad hoc by the organization. The outcome of this phase will be a **Target Profile**, i.e. the **desired reference, to which to aim and on which the assessment is carried out**.

The correct definition of this profile is therefore functional to the development of the next two phases.

Framework Methodology (2/3)

THREE PHASES



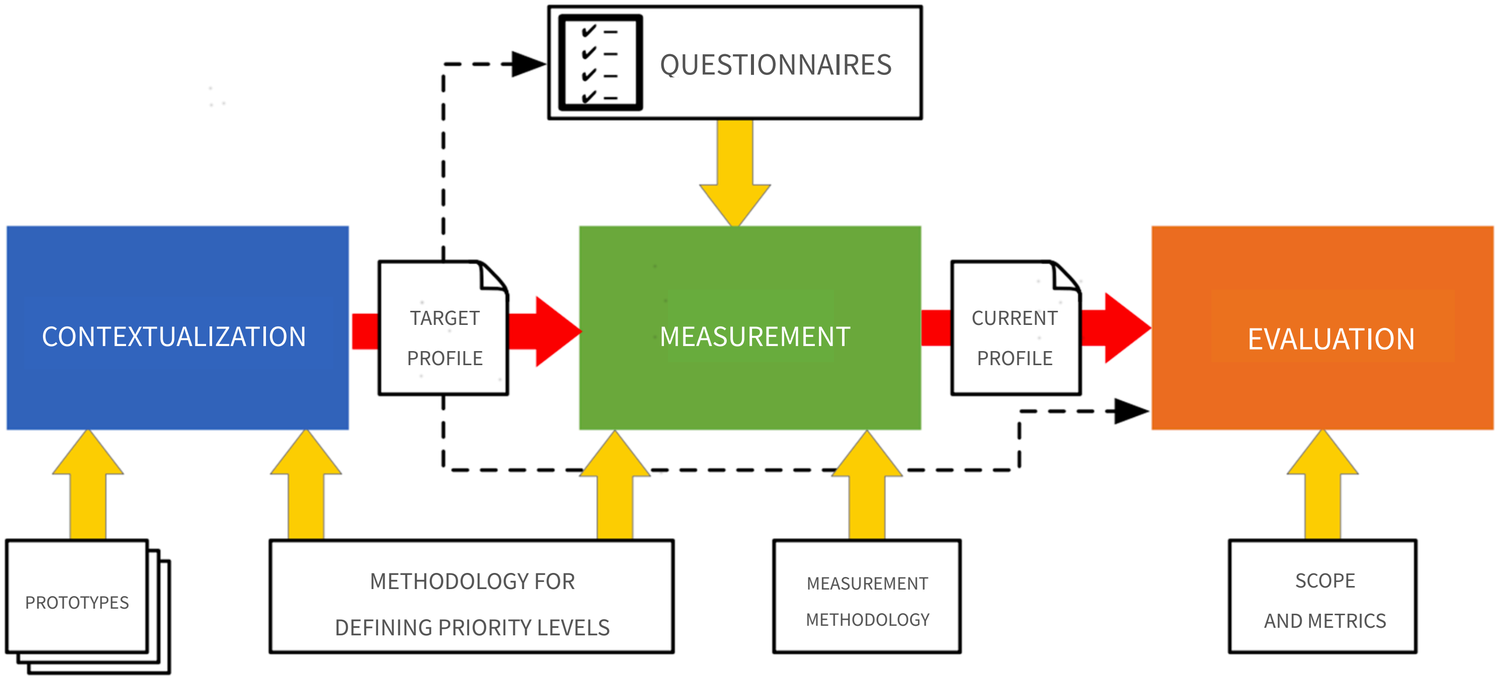
PHASE 2 - MEASUREMENT

In this second phase, the organization's current **cyber security posture** is identified against what is defined in the Target Profile.

This process is done through **interviews with relevant individuals** for the specific analysis needs. The result of the interviews is expressed in terms of coverage and maturity for each identified control.

Framework Methodology (3/3)

THREE PHASES



STEP 3 - EVALUATION

In the third phase, the results of the measurement phase are evaluated according to **several possible scopes**. This operation **allows to calculate,** starting from the values of coverage and maturity of each subcategory, **metrics of interest for the scope itself.** These metrics can consider, in an appropriately weighted way, the contributions of the various subcategories to the achievement of certain objectives for the scope itself, thus **allowing the results of the assessment to be analyzed from different points of view.**

Framework Outcomes and Scopes (1/2)

FINAL

The **output** of the **evaluation phase**, and therefore the result of the entire assessment, is **expressed through the metrics defined in the Framework**, aggregated according to different criteria and projected onto different **scopes** (e.g. risk management, compliance, etc.).

Scopes allow the assessment results to be interpreted from different perspectives within the organization.

Framework Outcomes and Scopes (2/2)

FINAL

SCOPE FRAMEWORK

This scope allows you to **assess how far the organization's current cyber security posture is from the goals set by the Target Profile**.

RISK MANAGEMENT SCOPE

This scope allows you to **analyze how consistent the organization's current cyber security posture is with respect to the risk mitigation** objectives associated with the threats to which the organization itself is exposed.

COMPLIANCE SCOPE

This scope allows you to assess how well the **Current Profile is aligned with the cybersecurity requirements of the industry in which the organization operates.**

OWASP: Web Security

TO SECURE THE WEB

The **Open Web Application Security Project® (OWASP)** is a **nonprofit foundation that works to improve the security of software.** Through community-led open-source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web.

- **OWASP Top 10**
- **OWASP Cheat Sheet**
- **OWASP Mobile Top 10**
- **OWASP Risk Rating Methodology**

OWASP Top 10!

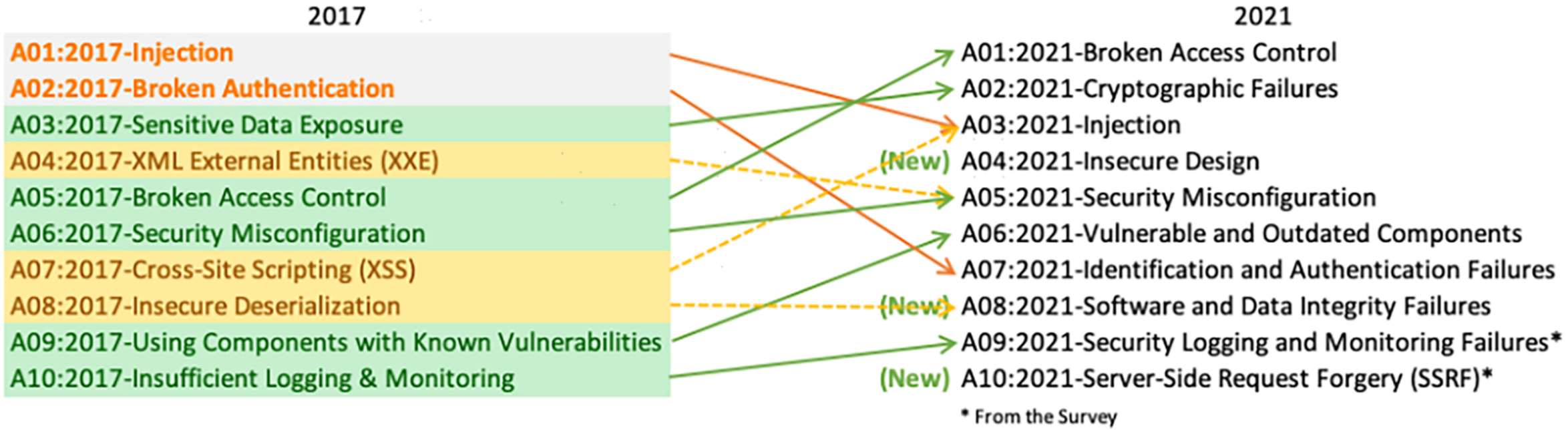
WEB APPLICATIONS

- The **OWASP Top 10** is a **standard awareness document for developers and web application security.** It represents a broad consensus about **the most critical security risks to web applications.** Companies should adopt this document and start the process of ensuring that their web applications minimize these risks.

- Using the OWASP Top 10 **is perhaps the most effective first step towards changing the software development culture** within your organization into one that produces more secure code.

OWASP Top 10!

WEB APPLICATIONS



The **OWASP Top 10** is an awareness document that highlights the **top 10 most critical web application security risks**.

The risks are in a ranked order based on frequency, severity, and magnitude for impact.

OWASP has maintained this list since 2003, and every few years, they update the list based on advancements in both application development and application security.

https://owasp.org/Top10/

OWASP Cheat Sheet Series

The OWASP Cheat Sheet Series was created to **provide a set of simple good practice guides for application developers and defenders to follow**.

Rather than focusing on detailed best practices that are impractical for many developers and applications, OWASP **Cheat Sheet Series is intended to provide useful practices that most developers will actually be able to implement**.

https://cheatsheetseries.owasp.org/

OWASP Mobile Top 10 [2016]

OWASP Mobile Top 10 consists of **the most critical security risks to mobile applications**. It represents a broad consensus about the most critical security risks to mobile applications.

In 2015, OWASP performed a survey and initiated a Call for Data submission globally. This helped them to analyze and recategorize the OWASP Mobile Top Ten for 2016. In this way, the top ten categories were more focused on Mobile applications rather than the Server.

The **Top 10 Mobile Risks** included:

- M1: Improper Platform Usage
- M2: Insecure Data Storage
- M3: Insecure Communication
- M4: Insecure Authentication
- M5: Insufficient Cryptography
- M6: Insecure Authorization
- M7: Client Code Quality
- M8: Code Tampering
- M9: Reverse Engineering
- M10: Extraneous Functionality

OWASP Mobile Application Security (MAS)

The **OWASP Mobile Application Security (MAS)** flagship project provides a **security standard for mobile apps (OWASP MASVS)** and a **comprehensive testing guide (OWASP MASTG)** that covers the processes, techniques, and tools used during a mobile app security test, as well as an **exhaustive set of test cases that enables testers to deliver consistent and complete results.**

OWASP MASVS

Download the MASVS

OWASP MASTG

Download the MASTG

OWASP Mobile Application Security

The **OWASP Mobile Application Security Checklist** contains links to the MASTG test case for each MASVS requirement.

- **Security Assessments / Pentests:** ensure you're at least covering the standard attack surface and start exploring.
- **Standard Compliance:** includes MASVS and MASTG versions and commit IDs
- **Learn & practice your mobile security skills.**
- **Bug Bounties:** go step by step covering the mobile attack surface.

Mobile Application Security Verification Standard

OWASP MASTG v1.5.0 (commit: 3b9278f)
OWASP MASVS v1.4.2 (commit: 2a8b582)

OWASP Mobile Security Project

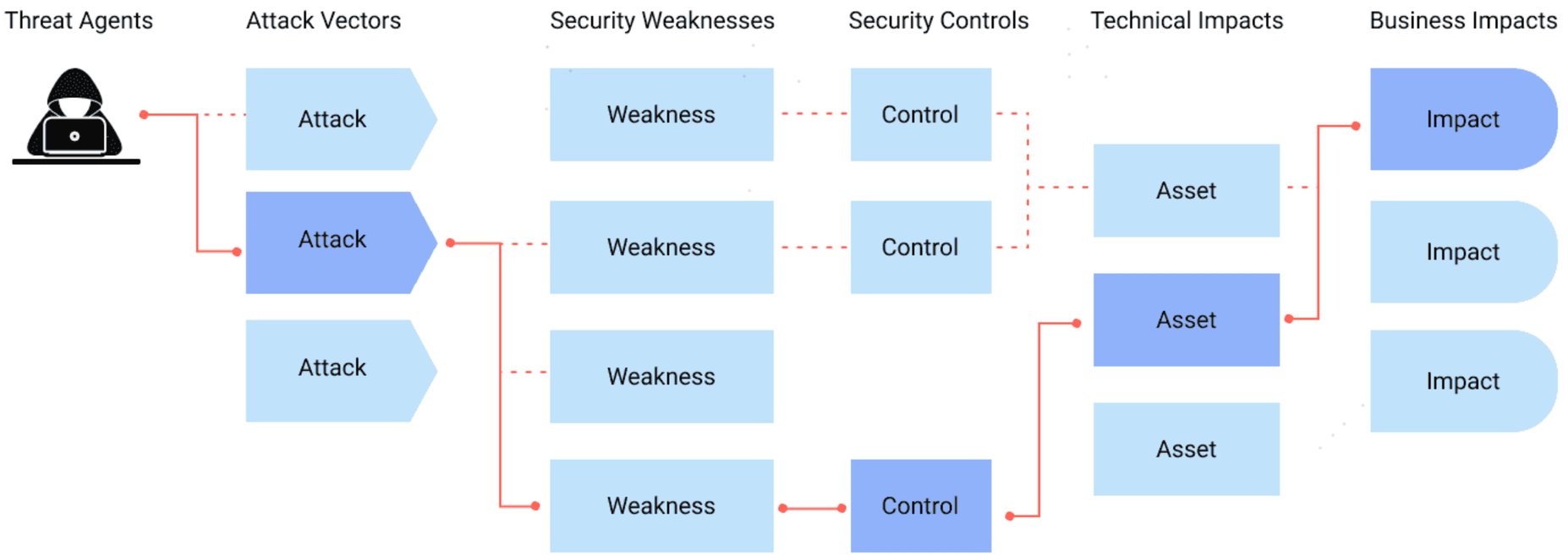
Data Storage and Privacy Requirements

ID	MASVS-ID	Detailed Verification Requirement	L1	L2	R	Common	Android	iOS	Status
2.1	MSTG-STORAGE-1	System credential storage facilities need to be used to store sensitive data, such as PII, user credentials or cryptographic keys.					Test Case	Test Case	Pass
2.2	MSTG-STORAGE-2	No sensitive data should be stored outside of the app container or system credential storage facilities.					Test Case	Test Case	Pass
2.3	MSTG-STORAGE-3	No sensitive data is written to application logs.					Test Case	Test Case	Fail
2.4	MSTG-STORAGE-4	No sensitive data is shared with third parties unless it is a necessary part of the architecture.					Test Case	Test Case	N/A
2.5	MSTG-STORAGE-5	The keyboard cache is disabled on text inputs that process sensitive data.					Test Case	Test Case	Pass
2.6	MSTG-STORAGE-6	No sensitive data is exposed via IPC mechanisms.					Test Case	Test Case	Fail
2.7	MSTG-STORAGE-7	No sensitive data, such as passwords or pins, is exposed through the user interface.					Test Case	Test Case	Fail
2.8	MSTG-STORAGE-8	No sensitive data is included in backups generated by the mobile operating system.					Test Case	Test Case	Fail

https://mas.owasp.org/MAS_checklist/

OWASP Risk Rating Methodology (1/2)

Attackers can take **a variety of routes through your application** to cause **damage** to your company or organization. Each of these routes entails a risk that may or may not be significant enough to attract attention.



OWASP Risk Rating Methodology (2/2)

OWASP Risk Rating Methodology is the procedure of following a path of several steps for the classification of threats. Let's have a look at these steps:

- **Step 1:** Identifying a Risk
- **Step 2:** Factors for Estimating Likelihood
- **Step 3:** Factors for Estimating Impact
- **Step 4:** Determining Severity of the Risk
- **Step 5:** Deciding What to Fix
- **Step 6:** Customizing Your Risk Rating Model

The process is very similar to what we've already seen!

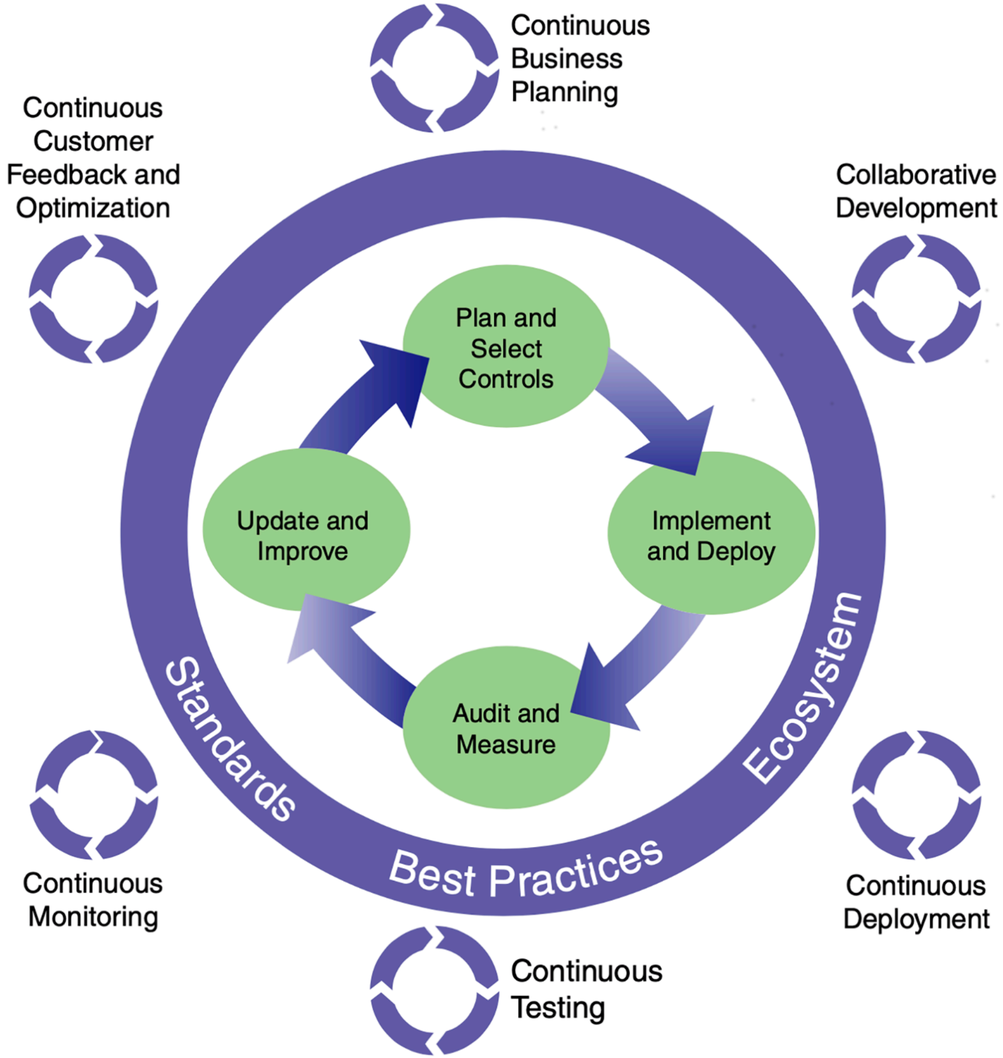
Contents

4. Effective Cybersecurity

- Management process
- Cybersecurity information and decision flow

Cybersecurity Management Process

EFFECTIVE CYBERSECURITY



An **essential** characteristic of cybersecurity provision is that it is **not a single end that is attained but an ongoing process.**

The goal of **effective cybersecurity** is constantly receding as **management makes an effort to keep up with changes in the cyberspace ecosystem**, which comprises technology, threat capability, applications, IT resources, and personnel.

Cybersecurity Information and Decision Flow

INSIDE AN ORGANIZATION

Two cyclic processes at work:

- one at the **executive level**, which focuses on organizational risk. At the executive level, upper management **defines** mission priorities, establishes acceptable risk tolerance, and determines available resources.
- one at the **business level**, which focuses on critical infrastructure risk management. At the business level, IT management **translates these guidelines into controls** for risk management.

SECURITY AND RISK: MANAGEMENT AND CERTIFICATIONS

Simone **Soderi**

simone.soderi@unipd.it

M1.2 - Basic Concepts

Thanks for your attention!