TOPIC 4
SECURITY POLICIES AND AUTOMATED HARDENING

Defense against the dark arts

José Manuel Redondo López *"S-81 Isaac Peral"* Project v4.0

Departamento de Informática
Universidad de Oviedo
Universidad de Oviedo

Logo: @creative_vanesa (*Instagram*)

INDEX

What is this topic?

- At the end of the previous topic, we outlined two key elements to achieve proper security with less effort
  - **Lists of validated, properly documented**, and maintained security controls
    - For any software product / OS we need to harden
  - A way to **automate their verification** and/or implement the solution to the vulnerabilities they resolve
- This topic will explore some sources of these lists and security automation technologies
  - Relating them to a much higher abstraction level elements
    - Like security policies, frameworks, and Information Security Management Systems (ISMS)
  - We will begin with the technical low-level part
    - And show the path up to the much more abstract security management techniques

< Go to Index

ENS >

SCAP >

Source: Bing Chat AI

SECURITY HARDENING AUTOMATION

Hardening could not be hard

*Icons by Bing Chat AI

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo

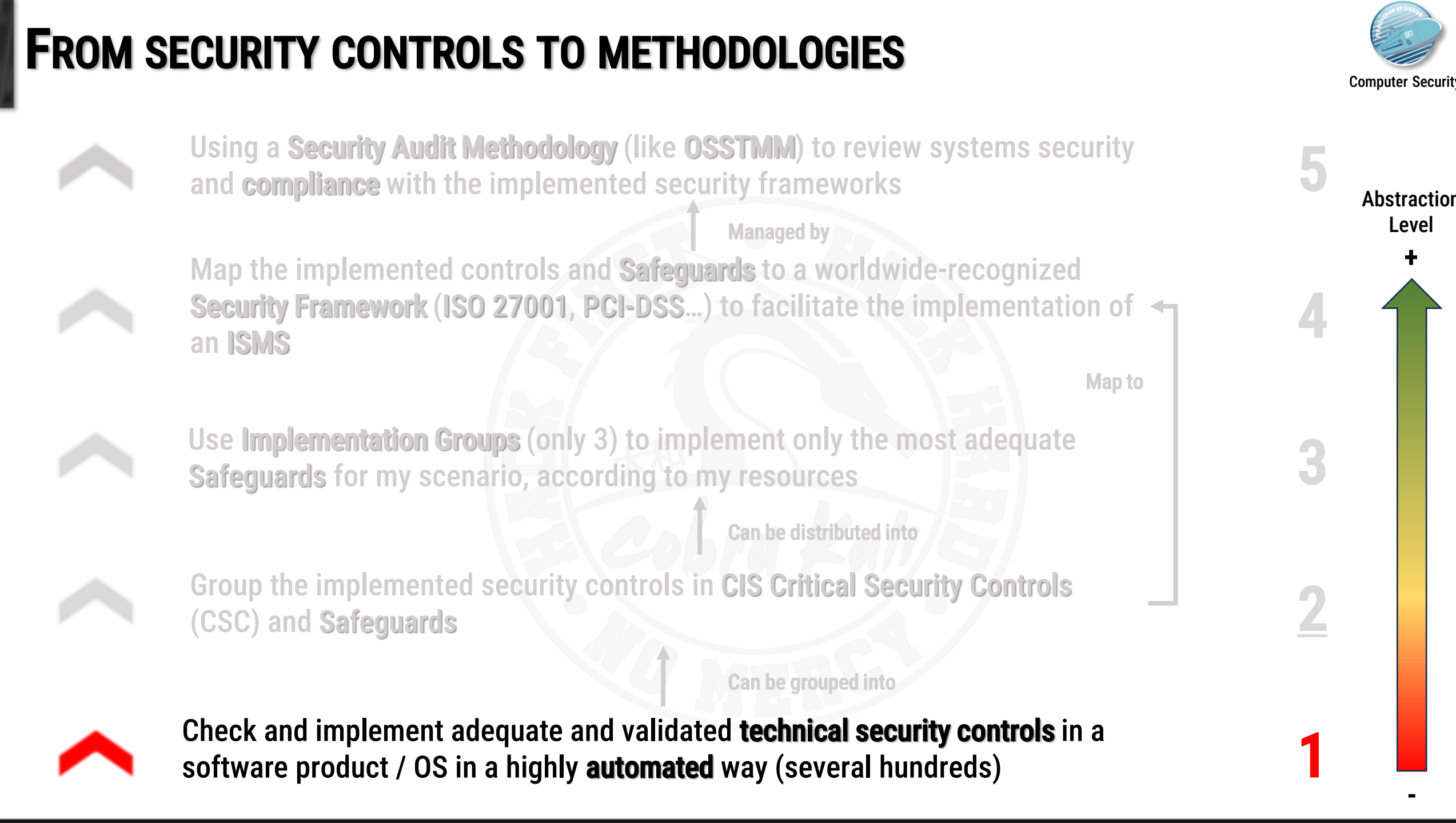
What are you going to find in this block?

- **In this block you will learn**
  - What the concept of **Compliance as Code** is
  - What is the National Security Scheme (**Esquema Nacional de Seguridad**) and what does it include
  - What is the **SCAP protocol** and what is it for, and its importance to automate it

COMPLIANCE AS CODE

- **Tools and practices that allow embed the three core activities of compliance: Prevent, detect, remediate**
  - **Prevent** non-compliance by automatically asserting planned changes are compliant
  - **Detect** non-compliance through automated scanning, notifying when problems are identified
  - **Remediate** non-compliance by making immediate changes to the infrastructure to ensure the maximum level of compliance on all of it
- **Therefore, it is the codification of our security controls**
  - So, their compliance, application and remediation **can be automated**
  - This applies to cybersecurity (**compliance controls are the security controls**)
  - In this topic we are going to review different ways of achieving this
  - And how this can be used to facilitate the implementation of security frameworks
- **This codification is done in special programming languages (Domain-Specific Languages, DSL (TPP, DLP))**
  - We are software engineers! Programming languages are our bread and butter!

From security controls to methodologies



Spanish Esquema Nacional de Seguridad (ENS)

Law 11/2007 (22th June): Citizens electronic access to public services. Our country's security controls

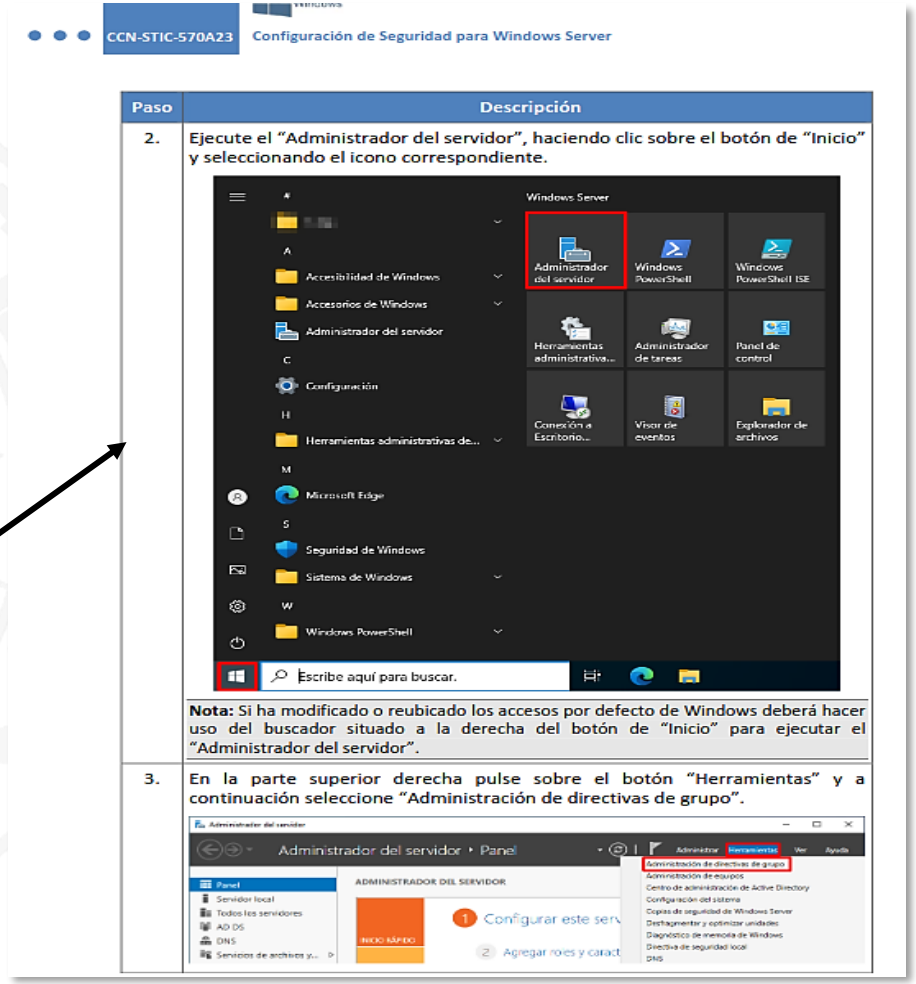
*Icons by Bing Chat AI

Esquema Nacional de Seguridad (Spain)

Computer Security

- **Establish the principles and requirements of a security policy to use electronic media**
  - **ENS Contents**: https://www.ccn-cert.cni.es/publico/ens/ens/index.html
  - **Regulatory framework**: https://ens.ccn.cni.es/es/ens-marco-normativo/ens-marco-normativo-es
- **To properly configure OS/Software**
  - The CCN-STIC publish **free security guides** for many products with security control lists
    - And step-by-step detailed explanations about each one
    - If you want an **extremely detailed manual with screen captures**, you will have an exceptional example here
  - They are organized in series in: https://www.ccn-cert.cni.es/es/guias.html
    - Windows (series **500**), Other OS (series **600**), Software (series **800**)…
  - **Recently updated**: https://www.linkedin.com/pulse/esquema-nacional-de-seguridad-ens-un-a%C3%B1o-despu%C3%A9s-su-actualizaci%C3%B3n/?originalSubdomain=es

Guides are created for public administrations, but private companies can use them too



Source: https://www.ccn-cert.cni.es/es/guias-de-acceso-publico-ccn-stic/7104-ccn-stic-570a23-perfilado-de-seguridad-para-windows-server-controlador-de-dominio-o-servidor-miembro/file.html

Esquema Nacional de Seguridad (Spain)

- **ENS defines profiles for the security controls**
  - But they are different for each SO/software
  - There is no homogeneity*, as in other solutions (Ex.: CSC Controls)
- **For Windows three profiles are defined**
  - Based on the classification of the data handler by the information systems
  - **ESTÁNDAR**, **USO OFICIAL,** and **MATERIAS CLASIFICADAS**
- **These three profiles may contain different configurations depending on the category of the information systems**
  - Defined in the ENS specification
  - **BÁSICA**, **MEDIA**, **ALTA**, and **SISTEMAS CLASIFICADOS**

***Red Hat** systems, for example, use a much different classification

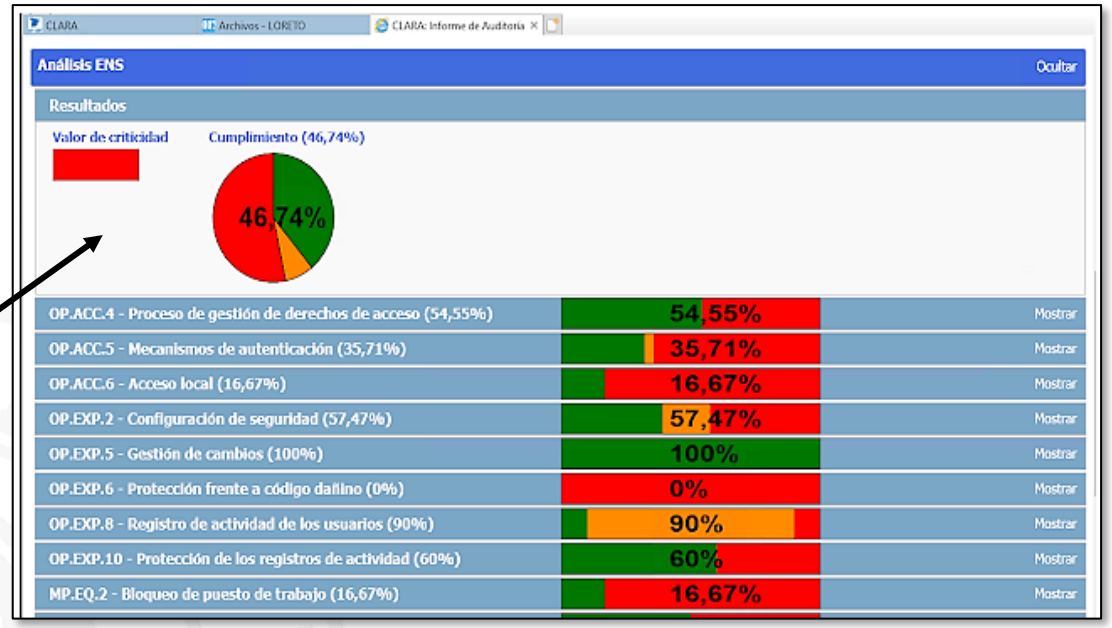
		CALIFICACIÓN DE LA INFORMACIÓN/PERFIL		
		ESTÁNDAR	USO OFICIAL	MATERIAS CLASIFICADAS
CATEGORÍA DEL SISTEMA DE INFORMACIÓN	BÁSICA	✓	✗	✗
	MEDIA	✓	✓	✗
	ALTA DIFUSIÓN LIMITADA	✗	✓	✗
	CONFIDENCIAL RESERVADO	✗	✗	✓

Applicable profiles depending on the category of the information systems to which they will be applied. Note that, for example, a USO OFICIAL profile can be applied to systems classified as MEDIA or ALTA

Esquema Nacional de Seguridad (Spain)

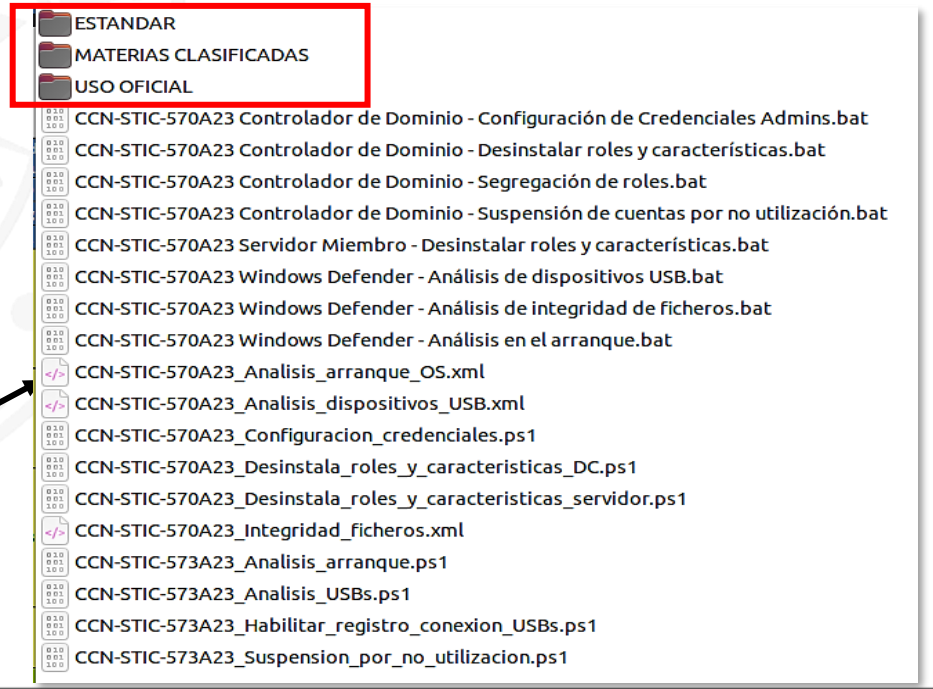
Computer Security

- **CCN-CERT also offers security software to their partners (or free)**
  - https://www.ccn-cert.cni.es/soluciones-seguridad.html
  - One is CLARA, a free an automated ENS-compliance checking tool for Windows and CentOS
  - **Tutorial**: http://kinomakino.blogspot.com/2020/08/si-quieres-auditar-tu-windows-y-no-lo.html



- **But ENS does not facilitate compliance as code**
  - They are not structured as other solutions
    - Problem - description - checking - remediation
    - They are designed to **require manual intervention**
  - Automated remediation measures are scripts
    - `.sh`, `.bat`, `.ps1`... files
    - **They do not follow international security automation standards** (SCAP)
    - They are executed inside some of the steps of its related step-by-step security guide

Scripts adapted to the profiles of the previous slide



Security Content Automation Protocol (SCAP)

Standardized automation protocol for hardening operations that facilitate Compliance as Code

*Icons by Bing Chat AI

Security Content Automation Protocol (SCAP)

- **NIST standard that allows automated hardening on software systems**
  - SCAP-compatible tools load files built in two XML-based markup language formats
    - **OVAL** and **XCCDF**
  - These files are used to automate
    - Security controls **evaluation** (see if each control is already applied)
    - And their **remediation** (apply the security control to solve the associated vulnerabilities)
  - Opposite to ENS, **all the operations are specified in processable XML files**
    - Not in a PDF guide and scripts linked to it
- **The OpenSCAP project is its most popular implementation**
  - A set of open-source tools complying with SCAP 1.2 : https://www.open-scap.org/
    - https://static.open-scap.org/openscap-1.3/oscap_user_manual.html
  - These tools allow
    - Automated configuration, checking for vulnerabilities, and patches
    - Technical security control compliance activities
    - Measuring the current security level
  - Opposite to ENS, it is possible to create tools that read and use these XML (**open standard**)

AUTOMATED HARDENING LANGUAGES

Computer Security

Source: https://www.ipa.go.jp/security/english/vuln/OVAL_en.html

Open Vulnerability Assessment Language (OVAL)

- https://oval.mitre.org/language/
- XML-based language created by MITRE (https://www.mitre.org/)
- Allows to **represent the information** of the different elements that form the configuration of a computer system
  - It also allows to analyze and evaluate these elements
  - To detect if a machine is in a certain state (vulnerability, configuration, patch level…)
- It allows to create a **report** with the evaluation results

```
<?xml version="1.0" encoding="UTF-8" ?>
 <oval_definitions>
  <definitions>
   <definition id="oval:jp.jvn.jvndb.oval:def:20091130"
   class="vulnerability" version="1">
    <metadata>
     <title>MyJVN バージョンチェッカの セキュリティチェック</title>
    </metadata>
    <criteria operator="AND">
     <criterion comment="MyJVN バージョンチェッカが最新 かどうかのテスト項目 "
     test_ref="oval:jp.jvn.jvndb.oval:tst:20091130" />
    </criteria>
   </definition>
  </definitions>
```

Tests element

```
<tests>
 <registry_test id="oval:jp.jvn.jvndb.oval:tst:20091130"
 version="1" comment="レジストリCurrentVersion値が1.0であれば最新である"
 check_existence="at_least_one_exists" check="at least one"
 xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows">
  <object object_ref="oval:jp.jvn.jvndb.oval:obj:1111" />
  <state state_ref="oval:jp.jvn.jvndb.oval:ste:2222" />
 </registry_test>
</tests>
```

Objects element

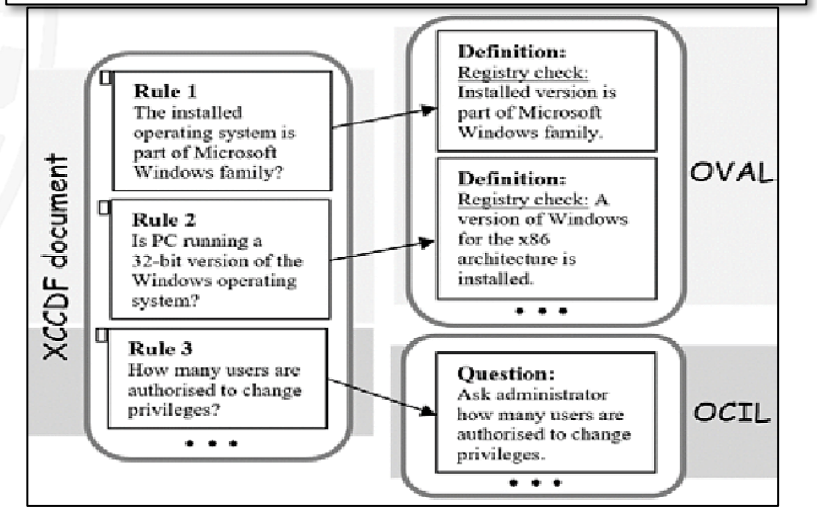
```
<objects>
 <registry_object id="oval:jp.jvn.jvndb.oval:obj:1111"
 version="1" xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows">
  <hive>HKEY_LOCAL_MACHINE</hive>
  <key>SOFTWARE¥IPA¥MyJVN</key>
  <name>CurrentVersion<name />
 </registry_object>
</objects>
```

States element

```
<states>
 <registry_state id="oval:jp.jvn.jvndb.oval:ste:2222"
 version="1" xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows">
  <value>1.0</value>
 </registry_state>
</states>
</oval_definitions>
```

Extensible Configuration Checklist Description Format (XCCDF)

- https://csrc.nist.gov/projects/security-content-automation-protocol/specifications/xccdf
- Another XML-based language specification created by NIST
- It allows writing **security controls lists**, security benchmarks and other related documents



Source: https://www.researchgate.net/figure/XCCDF-sample-use-case-scenario_fig3_311447068

AUTOMATED HARDENING LANGUAGES

Computer Security

Source Data Stream

- https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security_guide/sect-scap_format-data_stream
- File format compatible only with the SCAP protocol 1.2+
- It **bundles** XCCDF, OVAL, and other component files together
  - To define a compliance policy expressed in a XCCDF checklist
- It is also XML-based and contains an **index**, a **catalog**, and a **table of contents**
  - That allow splitting it into files according to the SCAP components (there can be multiple of the same type)
  - Covering all security policies needed in an organization
- It is the recommended format to use, if available, as it should be more complete that the other two
- It has its own editing tool, SCAP Composer
  - https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8290.pdf

```
<ds:data-stream-collection xmlns:ds="http://scap.nist.gov/schema/scap/source/1.2"
    xmlns:xlink="http://www.w3.org/1999/xlink"
    xmlns:cat="urn:oasis:names:tc:entity:xmlns:xml:catalog"
    id="scap_org.open-scap_collection_from_xccdf_ssg-rhel6-xccdf-1.2.xml"
    schematron-version="1.0">
  <ds:data-stream id="scap_org.open-scap_datastream_from_xccdf_ssg-rhel6-xccdf-1.2.xml"
      scap-version="1.2" use-case="OTHER">
  <ds:dictionaries>
    <ds:component-ref id="scap_org.open-scap_cref_output--ssg-rhel6-cpe-dictionary.xml"
        xlink:href="#scap_org.open-scap_comp_output--ssg-rhel6-cpe-dictionary.xml">
      <cat:catalog>
        <cat:uri name="ssg-rhel6-cpe-oval.xml"
            uri="#scap_org.open-scap_cref_output--ssg-rhel6-cpe-oval.xml"/>
      </cat:catalog>
    </ds:component-ref>
  </ds:dictionaries>
  <ds:checklists>
    <ds:component-ref id="scap_org.open-scap_cref_ssg-rhel6-xccdf-1.2.xml"
        xlink:href="#scap_org.open-scap_comp_ssg-rhel6-xccdf-1.2.xml">
      <cat:catalog>
        <cat:uri name="ssg-rhel6-oval.xml"
            uri="#scap_org.open-scap_cref_ssg-rhel6-oval.xml"/>
      </cat:catalog>
    </ds:component-ref>
  </ds:checklists>
  <ds:checks>
    <ds:component-ref id="scap_org.open-scap_cref_ssg-rhel6-oval.xml"
        xlink:href="#scap_org.open-scap_comp_ssg-rhel6-oval.xml"/>
    <ds:component-ref id="scap_org.open-scap_cref_output--ssg-rhel6-cpe-oval.xml"
        xlink:href="#scap_org.open-scap_comp_output--ssg-rhel6-cpe-oval.xml"/>
    <ds:component-ref id="scap_org.open-scap_cref_output--ssg-rhel6-oval.xml"
        xlink:href="#scap_org.open-scap_comp_output--ssg-rhel6-oval.xml"/>
  </ds:checks>
</ds:data-stream>
<ds:component id="scap_org.open-scap_comp_ssg-rhel6-oval.xml"
    timestamp="2014-03-14T16:21:59">
  <oval_definitions xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5"
      xmlns:oval="http://oval.mitre.org/XMLSchema/oval-common-5"
      xmlns:ind="http://oval.mitre.org/XMLSchema/oval-definitions-5#independent"
      xmlns:unix="http://oval.mitre.org/XMLSchema/oval-definitions-5#unix"
      xmlns:linux="http://oval.mitre.org/XMLSchema/oval-definitions-5#linux"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:schemaLocation="http://oval.mitre.org/XMLSchema/oval-common-5
      oval-common-schema.xsd
          http://oval.mitre.org/XMLSchema/oval-definitions-5
      oval-definitions-schema.xsd
          http://oval.mitre.org/XMLSchema/oval-definitions-5#independent
      independent-definitions-schema.xsd
          http://oval.mitre.org/XMLSchema/oval-definitions-5#unix
      unix-definitions-schema.xsd
          http://oval.mitre.org/XMLSchema/oval-definitions-5#linux
      linux-definitions-schema.xsd">
```

Security Content Automation Protocol (SCAP)

- So, this protocol and its XML languages are a worldwide standard to
  - **Check software configurations**, **manage vulnerabilities**, and **evaluate** if a system complies with a particular security policy, all with a **high degree of automation**
- **All using documented and validated procedures to minimize errors**
  - **Automatically evaluating security controls application** (*is this already done?*)
  - **Automatic remediation of security controls** (if the answer is no, resolve it)
  - **Generating a report with the results of the evaluation / remediation** (typically, HTML)
- **OpenSCAP** is a tool that does this, but many more could exist!
- More information
  - **SCAP security policies**: https://www.open-scap.org/security-policies/
  - **OpenSCAP user manual**: https://static.open-scap.org/openscap-1.2/oscap_user_manual.html
  - **Documentation, user manuals, and security guidelines for several OS**: https://static.open-scap.org/
- ***Do you understand now the difference with the ENS proposal?***

CURRENT STATE OF SECURITY AUTOMATION

- So, **SCAP**, **OVAL** and **XCCDF** are a very important and ongoing effort to try to standardize and automate security processes
- There are files written in these languages that allow us to check or remediate security controls over a large amount of software / OS
  - Next section will review popular sources of these files
- These files usually include different **usage profiles** or **security policies**
  - A single file can contain different lists of security controls to check or remediate
  - Depending on how we are going to use the software (e. g.: server, workstation…)
  - The definition of what is a usage profile / security policy depends on the source of the files
- The problem is to find complete, validated, and SCAP-compatible security control lists for free for all software and OS we use
  - **ENS does not have this problem**: All is centralized in its web

Think you've understood it all? Evaluate yourself!

?

- **You can do the following**
  - *Understand that software security can be managed with code*
  - *Understand that such code can detect and fix configuration issues that may cause vulnerabilities in such software*
    - *And thanks to it we can automate all these tasks, so the system complies with a security standard*
  - ***About the ENS***
    - *Understand that they are a series of principles and security requirements of our country*
    - *You know about what their security guides include, and what you can use them for*
    - *You understand that not all machines in an infrastructure are treated with equal importance and there are three usage profiles and four configuration categories*
    - *You know what you can use the ENS CLARA tool for*
  - ***About SCAP***
    - *You understand that it's based on three XML vocabularies: OVAL, XCCDF, and Source Data Stream*
    - *You understand that, thanks to the SCAP protocol, you can evaluate systems, detect which security controls are missing from implementation and remediate them*
      - *As well as generating a report on how the system is doing in terms of implementing controls*
    - *You know that, without a proper list of security controls, the SCAP protocol alone doesn't do anything to improve security*

< Go to Index

SOURCES OF VALIDATED SECURITY CONTROL LISTS

Some sources to obtain adequate technical guidelines (security control lists) for our products

*Icons by Bing Chat AI

Source: Bing Chat AI

SCAP Sec. Guide >

STIGs >

CIS Benchmarks >

WHAT ARE YOU GOING TO FIND IN THIS BLOCK?

- **In the first section of this block, you will learn**
  - What's included in the **scap-security-guide** package and its security profiles
  - The different ways to **use the files** included
  - What the **security reports** that are obtained when using the SCAP protocol are
- **In the next one, you'll learn**
  - Where do **STIG** standards and their military character come from
  - The **criteria** used to subdivide STIG security controls
  - Where you can **download STIG for free** and how to navigate them
  - The different parts of the definition of a **STIG security control** and what they mean
- **And finally, in the last section of this block you will learn**
  - What **CIS security controls** are and who endorses them
  - That all implementation instructions and their justification are **freely available in PDF format**
  - The **general structure** of any CIS control
  - How to achieve free and **automatic CIS compliance** with official and 3rd grade tools

The SCAP Security Guide package (`scap-security-guide`)

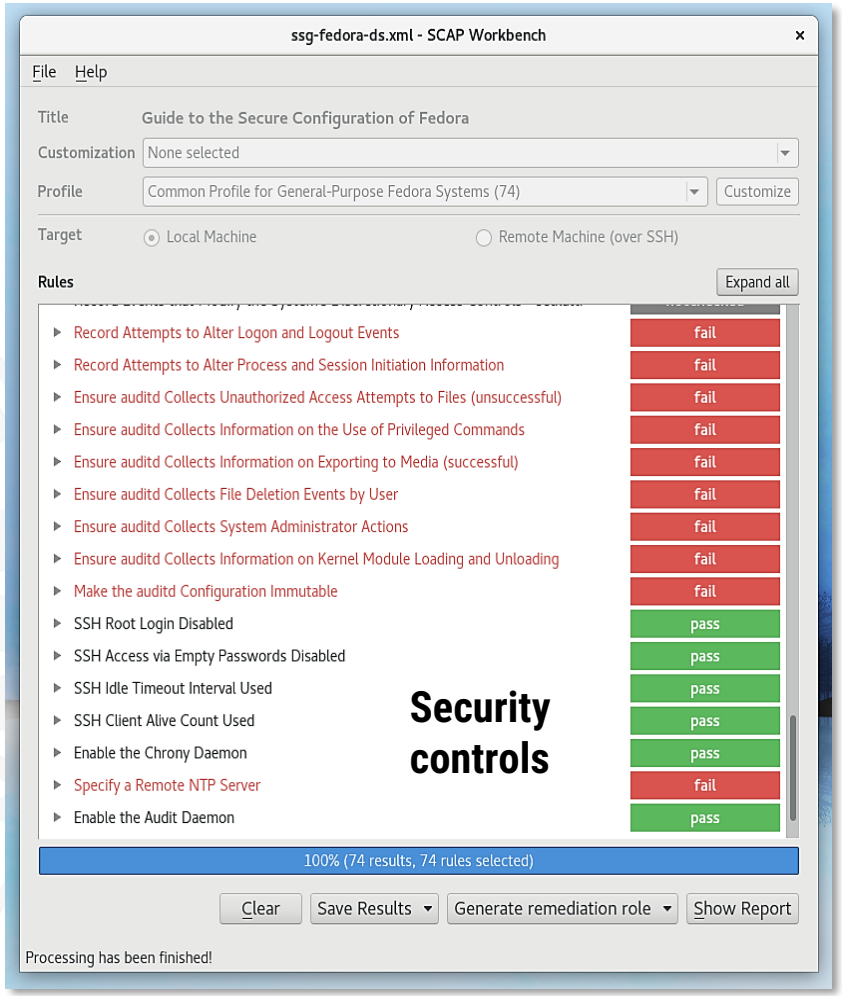
An easy way to find a free and trustable security control source

***Icons by Bing Chat AI**

THE SCAP-SECURITY-GUIDE PACKAGE

https://www.open-scap.org/security-policies/scap-security-guide/

- **OpenSCAP should be also partnered with free and open files required to secure software systems**
- **This package covers this requirement, containing**
  - **The `oscap` tool** (the OpenSCAP implementation)
  - **A set of SCAP-compatible preconstructed security policies**
    - With security controls applicable to several software products / OS (Red Hat, Fedora, Ubuntu,…)
    - Using these files, we can attain higher security levels than default installations with little effort
    - Not every security control contained in these files can be remediated using OpenSCAP (yet)
    - Support for remediation also improves as development of the SCAP files continues
    - They are created using parts of other security recommendations we will review (CIS, STIG…)

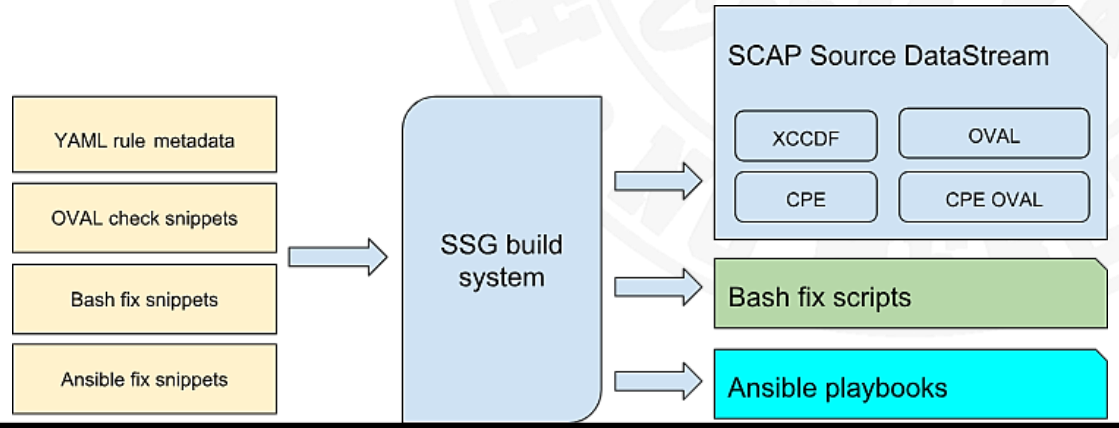


SCAP Workbench is a GUI for `openscap`, if you don't want to use the command line:
https://static.open-scap.org/scap-workbench-1.1/

➢ Exercise **L6B1_OSCAPUPD**

The scap-security-guide package: Remediation

- **Keeping this package updated improves and extends its security controls**
  - https://github.com/ComplianceAsCode/content
- **There are three forms of automated remediation**
  - **Using the SCAP files** with the OpenSCAP tool
  - Ansible playbooks (https://www.ansible.com/, sets of directories and `.yml` files)
    - Ansible is an automatic Windows and/or Linux infrastructure configuration tool
    - If we have SSH access to the machines, it can be used to **secure multiple machines in the same operation**
  - **Bash scripts**: meant to be run on machines to put them into compliance with a policy
    - They do not require to install anything (not OpenSCAP, not Ansible…) these Linux scripts just run
  - This way you have options for any machine you want to harden



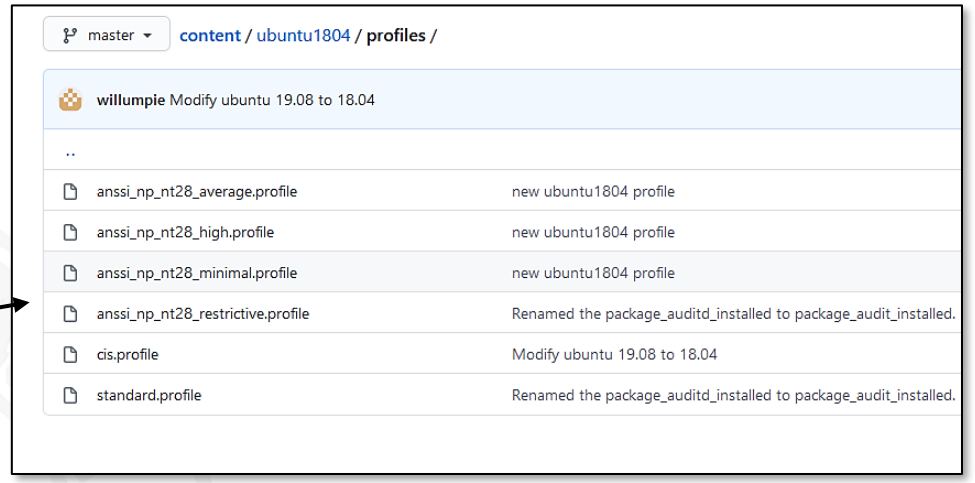
There are three ways to do remediation, and you choose which one suits you best. Some remedy more controls than others, although they start from the same base. Bash scripts can be copied to any machine to run them. Be very careful with automatic remediation: It could break some legitimate service

➢ Exercises **L6B2_OSCAPREMWB, L6B2_OSCAPREMBASH, L6B2_OSCAPREMANS**

The scap-security-guide package: Security profiles

Computer Security

- **The image shows the SCAP security profiles of the for the Ubuntu 18.04 OS**
  - A standard security profile, representing a minimum-security baseline that every Ubuntu should comply
  - Four profiles from the French security regulation ANSSI DAT-NT28
  - A security profile based on the CIS benchmarks security control lists (reviewed later)
- **The 2nd image shows the execution of the bash content related to the `standard` profile**
  - Each profile has its Ansible and bash script associated
  - Remember: The profiles are used with `openscap`, but if you don't (or can't) use it, there are more options!



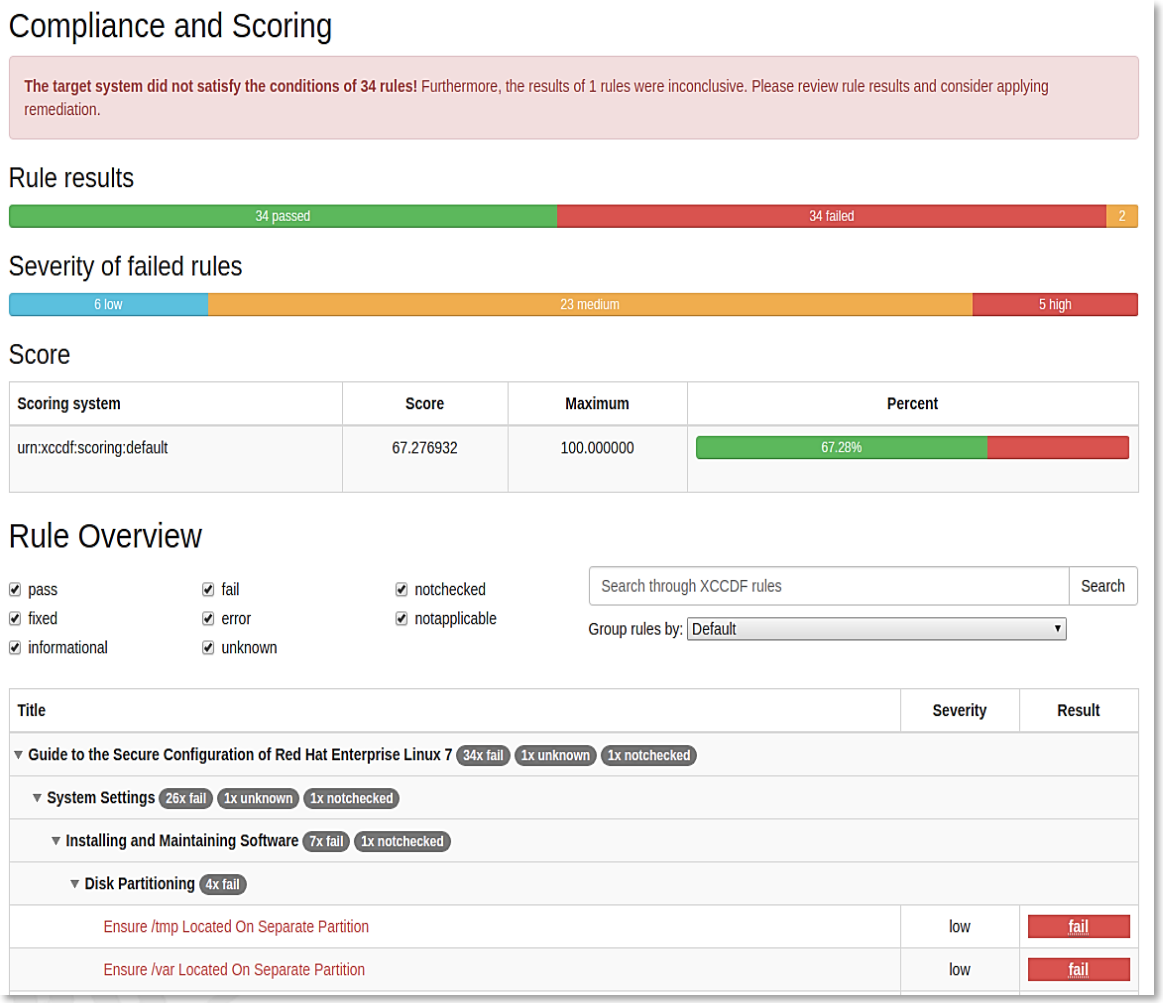
SCAP- compatible files (profiles)

```
operario@server1804:/etc/oscap/content/bash$ sudo bash ubuntu1804-script-standard.sh
Remediating rule 22/45: 'package_rsyslog_installed'
FIX FOR THIS RULE 'package_rsyslog_installed' IS MISSING!
Remediating rule 23/45: 'service_rsyslog_enabled'
FIX FOR THIS RULE 'service_rsyslog_enabled' IS MISSING!
Remediating rule 24/45: 'file_groupowner_etc_group'
Remediating rule 25/45: 'file_groupowner_etc_gshadow'
Remediating rule 26/45: 'file_groupowner_etc_passwd'
Remediating rule 27/45: 'file_groupowner_etc_shadow'
Remediating rule 28/45: 'file_owner_etc_group'
Remediating rule 29/45: 'file_owner_etc_gshadow'
Remediating rule 30/45: 'file_owner_etc_passwd'
Remediating rule 31/45: 'file_owner_etc_shadow'
Remediating rule 32/45: 'file_permissions_etc_group'
Remediating rule 33/45: 'file_permissions_etc_gshadow'
Remediating rule 34/45: 'file_permissions_etc_passwd'
Remediating rule 35/45: 'file_permissions_etc_shadow'
Remediating rule 36/45: 'file_permissions_systemmap'
FIX FOR THIS RULE 'file_permissions_systemmap' IS MISSING!
```

➢ Exercises **L6B1_OSCAPAUDITSW, L6B1_OSCAPAUDITSO, L6B1_OSCAPCMD**

The scap-security-guide package: Security reports

- The `oscap` tool can be run with the `eval` parameter to create an HTML report
  - This is the **evaluation-only** mode
  - It can be run with `--remediate` to try to **remediate** the not yet implemented controls
- The HTML report of an analyzed system contains
  - **The number of security controls** that the system already implements, those that don't, and those that are undetermined
    - A few require manual checking
  - Of those who no, it details its **severity**
    - Shows the importance of the lack of security controls
  - It shows a compliance % (**security score**)
  - And finally, a detailed list of each control
    - Whose entries can be opened to know its details



It is very interesting to create a report before remediation and another after doing it, to compare scores and what has been automated with these tools

Advantages / disadvantages

Advantages

- Available for **free**
- **Substantially increase the base security level** of a newly installed compatible software with little effort, facilitating Compliance as Code
- Frequently **maintained and improved,** being easily **updatable**
- *Do you have SCAP 1.2 compatible files for other places?* You can validate / perform its contained remediation procedures with OpenSCAP
  - Some only validate controls, and others are created to perform a manual processing of both tasks
  - They are mete lists of task to do to comply with a given security profile
  - ¡Maybe you **can use the step-by-step guides of the ENS** to implement these manual tasks!

Disadvantages

- **Incomplete** for some products, or remediation is not available for several controls
- **Supports much less software products** than other options (basically, only Linux OS)
- **They are not as validated** as the other security control sources, as they are not backed up by governments / private companies

Think you've understood it all? Evaluate yourself!

?

- **You can do the following**
  - *Understand that the **scap-security-guide** package is basically a free and open source of security checklists for certain OS*
  - *Know that, as part of that package, is included a simple GUI to apply them, **oscap**, which is an alternative to using them on the command line*
  - *Understand that not all included security controls have OSCAP remediation in place*
    - *But that remediation can also be implemented in the **Ansible** and/or **bash** files that are also included in the package*
  - *Understand that each distributed SCAP file may have different security profiles applicable to the product it is working on*
    - *And that these profiles change depending on the product*
  - *Be clear about the structure of a SCAP report generated on an evaluated software, where its overall security index is and the controls it passes and does not pass*

Security Technical Implementation Guides (STIGs)

Security control lists to make your software great again ☺

*Icons by Bing Chat AI

National Institute of Standards and Technology (NIST)

https://www.nist.gov/

- **Agency of the U.S. Department of Commerce**
  - **Free and public STIG archive**: 560+ security benchmarks for many products
    - Benchmarks are basically **security control lists**
    - A lot of them are also SCAP-compatible: https://public.cyber.mil/stigs/scap/
    - Each benchmark is a detailed guide on how to properly configure an OS, application, software...
  - They are free because civilian companies that gain public contracts with the US government can be required to provide software systems that comply with certain STIGs
- **STIG is one of the configuration standards used by the US Department of Defense (DoD) and DISA (Defense Information Systems Agency)**
  - Therefore, they could be considered military-grade security guidelines
- **Also publishes the SP 800-115**
  - Technical Guide to Information Security Testing and Assessment
  - Assist organizations in planning and conducting technical security tests & examinations
  - Analyzing findings, and developing mitigation strategies:
    - https://csrc.nist.gov/publications/detail/sp/800-115/final
  - **Description**: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-70r4.pdf

STIG CATEGORIES

- Categories are applied to security controls
- For each type of device or application, a STIG contains **hundreds of controls** to determine if they meet the security standard specified by it
  - For example, a Windows Server STIG specifies how to configure the password, assign permissions to users, configure auditing...
- Each of the controls in a STIG is assigned a severity level
  - **CAT I**: If not remediated, it can trigger a vulnerability whose exploitation directly causes a loss of confidentiality, availability or integrity (**very serious**)
  - **CAT II**: If not remediated, it can trigger a vulnerability whose exploitation can potentially cause a loss of confidentiality, availability or integrity (**intermediate**)
  - **CAT III**: If not remediated, it can trigger a vulnerability whose exploitation causes a degradation of the measures that prevent loss of confidentiality, availability or integrity (**less severe**)

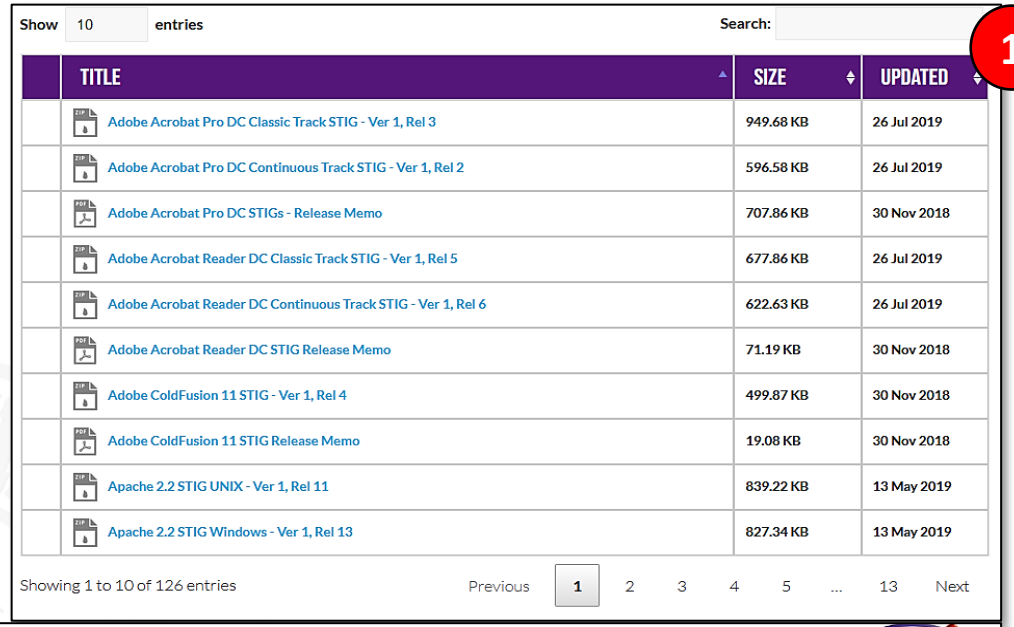
Mission Assurance Category (MACs) levels

- MACs are applied to machines / systems (same as ALTA, BAJA... in the ENS)
- **All systems** covered by STIGs are also classified based on **the importance of the information they manage, and how critical it is**
  - **MAC I**: Systems managing vital information to guarantee the effectiveness of its functionality
    - Losing one is unacceptable, they have the **strongest security measures**
  - **MAC II**: Systems managing important information for the performed functionality
    - Losing one is a major problem, implement **medium security measures**
  - **MAC III**: Systems that manage information necessary for daily system activity
    - But losing them do not affect to meet the functionality of the system in the short term
    - Losing one is acceptable, their security is based on **best management practices**
- There are also three levels to classify **information confidentiality**
  - Defined by the DoDI 8500.2: https://fas.org/irp/doddir/dod/d8500_2.pdf: **Classified**, **Sensitive**, **Public**
- MAC and confidentiality levels are independent
  - MAC I systems can handle public information, MAC III classified information…

Downloading STIGs

Computer Security

- We can download STIGs from multiple sources
  - **STIGs document library** (1)
    - https://public.cyber.mil/stigs/downloads
  - **National Checklist Program Repository** (2)
    - https://nvd.nist.gov/ncp/repository
    - Also contains links to many other third-party authorities SCAP-compatible files, not only STIGs
    - Even CIS Benchmarks (see next section)
  - **Third-party search engines**
    - https://cyber.trackr.live/stig
  - Some can also be found in the SCAP Security Guide package we saw

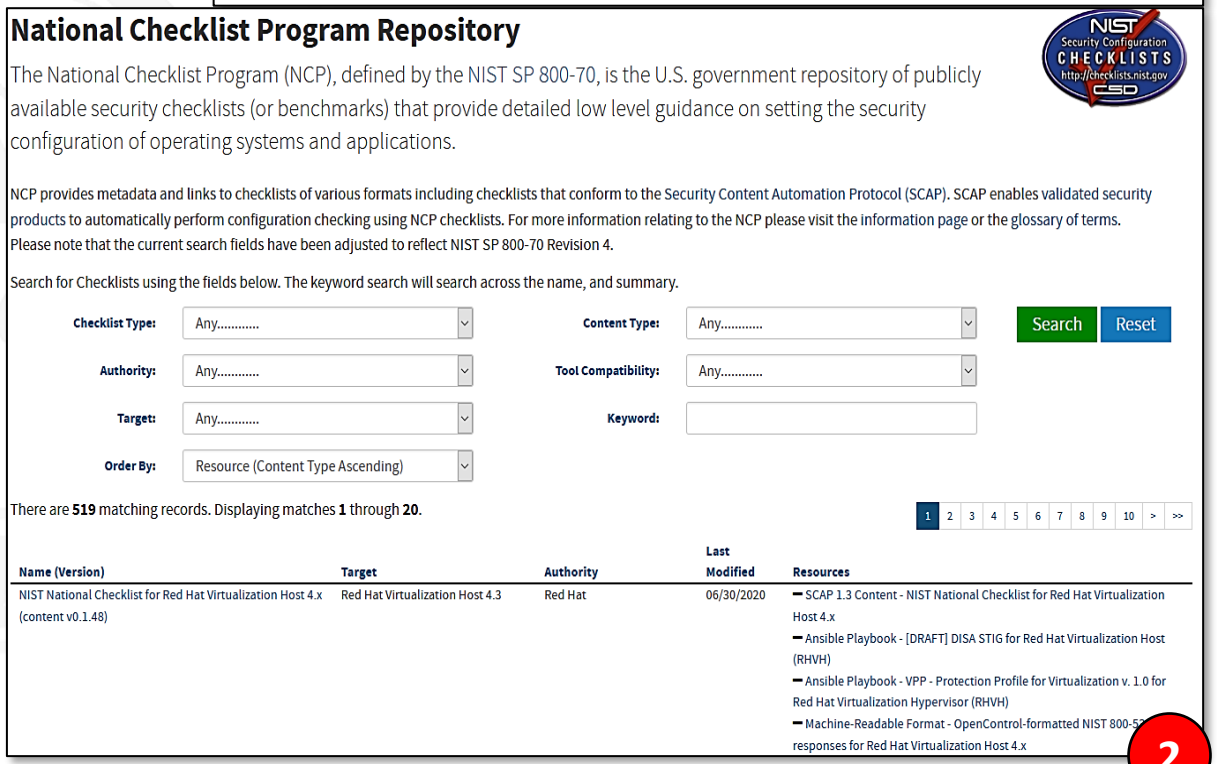


Show 10 entries Search:

TITLE	SIZE	UPDATED
Adobe Acrobat Pro DC Classic Track STIG - Ver 1, Rel 3	949.68 KB	26 Jul 2019
Adobe Acrobat Pro DC Continuous Track STIG - Ver 1, Rel 2	596.58 KB	26 Jul 2019
Adobe Acrobat Pro DC STIGs - Release Memo	707.86 KB	30 Nov 2018
Adobe Acrobat Reader DC Classic Track STIG - Ver 1, Rel 5	677.86 KB	26 Jul 2019
Adobe Acrobat Reader DC Continuous Track STIG - Ver 1, Rel 6	622.63 KB	26 Jul 2019
Adobe Acrobat Reader DC STIG Release Memo	71.19 KB	30 Nov 2018
Adobe ColdFusion 11 STIG - Ver 1, Rel 4	499.87 KB	30 Nov 2018
Adobe ColdFusion 11 STIG Release Memo	19.08 KB	30 Nov 2018
Apache 2.2 STIG UNIX - Ver 1, Rel 11	839.22 KB	13 May 2019
Apache 2.2 STIG Windows - Ver 1, Rel 13	827.34 KB	13 May 2019

Showing 1 to 10 of 126 entries Previous 1 2 3 4 5 ... 13 Next

1



National Checklist Program Repository

The National Checklist Program (NCP), defined by the NIST SP 800-70, is the U.S. government repository of publicly available security checklists (or benchmarks) that provide detailed low level guidance on setting the security configuration of operating systems and applications.

NCP provides metadata and links to checklists of various formats including checklists that conform to the Security Content Automation Protocol (SCAP). SCAP enables validated security products to automatically perform configuration checking using NCP checklists. For more information relating to the NCP please visit the information page or the glossary of terms. Please note that the current search fields have been adjusted to reflect NIST SP 800-70 Revision 4.

Search for Checklists using the fields below. The keyword search will search across the name, and summary.

Checklist Type: Any..... Content Type: Any..... Search Reset

Authority: Any..... Tool Compatibility: Any.....

Target: Any..... Keyword:

Order By: Resource (Content Type Ascending)

There are **519** matching records. Displaying matches **1** through **20**.

1 2 3 4 5 6 7 8 9 10 > >>

Name (Version)	Target	Authority	Last Modified	Resources
NIST National Checklist for Red Hat Virtualization Host 4.x (content v0.1.48)	Red Hat Virtualization Host 4.3	Red Hat	06/30/2020	– SCAP 1.3 Content - NIST National Checklist for Red Hat Virtualization Host 4.x – Ansible Playbook - [DRAFT] DISA STIG for Red Hat Virtualization Host (RHVH) – Ansible Playbook - VPP - Protection Profile for Virtualization v. 1.0 for Red Hat Virtualization Hypervisor (RHVH) – Machine-Readable Format - OpenControl-formatted NIST 800-53 responses for Red Hat Virtualization Host 4.x

2

Example. STIG "Canonical Ubuntu 20.04 LTS": Profiles

Source: https://www.stigviewer.com/stig/canonical_ubuntu_20.04_lts/

- **All controls in a STIG benchmark are grouped by its CAT classification**
  - We have 13 CAT I, 133 CAT II and 21 CAT III
- **Each STIG has 9 application profiles (3 confidentiality levels per MAC)**
  - Selecting one varies the number of controls to be performed on each CAT
  - And therefore, the length of the security control list to validate
- **We also have downloads**
  - XML/JSON files to automatically check whether this level is met **with proper tools**
  - An Excel file (`.csv`) to facilitate **manual checks**

Version	Date	Finding Count (167)			Downloads
1	2022-06-06	CAT I (High): 13	CAT II (Med): 133	CAT III (Low): 21	Excel JSON XML

STIG Description

This Security Technical Implementation Guide is published as a tool to improve the security of Department of Defense (DoD) information systems. The requirements are derived from the National Institute of Standards and Technology (NIST) 800-53 and related documents. Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil.

Available Profiles

Classified	Public	Sensitive						
I - Mission Critical Classified	I - Mission Critical Public	I - Mission Critical Sensitive	II - Mission Support Classified	II - Mission Support Public	II - Mission Support Sensitive	III - Administrative Classified	III - Administrative Public	III - Administrative Sensitive

Example: STIG "Canonical Ubuntu 20.04 LTS": Profile security control list

Computer Security

- **Once a MAC-confidentiality profile is chosen, the STIG presents the applicable list of security controls with**
  - **Finding ID**: Unique control ID
  - **Severity**: Severity of the associated vulnerability if discovered in the audited system
  - **Title**: Summary of the control objectives
  - **Description**: Detailed description of the effects or particularities of the control
- **By clicking into each security control, we can see its details**

Findings (MAC III - Administrative Sensitive)

Finding ID	Severity	Title	Description
V-238204	High	Ubuntu operating systems when booted must require authentication upon booting into single-user and maintenance modes.	To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must...
V-238206	High	The Ubuntu operating system must ensure only users who need access to security functions are part of sudo group.	An isolation boundary provides access control and protects the integrity of the hardware, software, and firmware that perform security functions. Security functions are the hardware, software,...
V-238201	High	The Ubuntu operating system must map the authenticated identity to the user or group account for PKI-based authentication.	Without mapping the certificate used to authenticate to the user account, the ability to determine the identity of the individual user or group will not be available for forensic analysis.
V-238363	High	The Ubuntu operating system must implement NIST FIPS-validated cryptography to protect classified information and for the following: to provision digital signatures, to generate cryptographic hashes, and to protect unclassified information requiring confidentiality and cryptographic protection in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	Use of weak or untested encryption algorithms undermines the purposes of utilizing encryption to protect data. The operating system must implement cryptographic modules adhering to the higher...
V-238219	High	The Ubuntu operating system must be configured so that remote X connections are disabled, unless to fulfill documented and validated mission requirements.	The security risk of using X11 forwarding is that the client's X11 display server may be exposed to attack when the SSH client requests forwarding. A System Administrator may have a stance in...
V-238218	High	The Ubuntu operating system must not allow unattended or automatic login via SSH.	Failure to restrict system access to authenticated users negatively impacts Ubuntu operating system security.

Source: https://www.stigviewer.com/stig/canonical_ubuntu_20.04_lts/2022-06-06/MAC-3_Sensitive/

STIG "Canonical Ubuntu 20.04 LTS": Individual control detailed information

Computer Security

- The description of each control tells us **how to verify and how to fix the detected problems**
- Therefore, they are validated, documented, and trustable ways of checking for potential vulnerabilities
  - And how to remediate them
- But **classified according to a military point of view**
  - The confidentiality and mission criticality of the computers

The Ubuntu operating system must use SSH to protect the confidentiality and integrity of transmitted information.

Overview

Finding ID	Version	Rule ID	IA Controls	Severity
V-238215	UBTU-20-010042	SV-238215r653820_rule		High

Description

Without protection of the transmitted information, confidentiality and integrity may be compromised because unprotected communications can be intercepted and either read or altered. This requirement applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, and facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification. Protecting the confidentiality and integrity of organizational information can be accomplished by physical means (e.g., employing physical distribution systems) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, then logical means (cryptography) do not have to be employed, and vice versa. Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000425-GPOS-00189, SRG-OS-000426-GPOS-00190

STIG	Date
Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide	2022-06-06

Details

Check Text (C-41425r653818_chk)

Verify the SSH package is installed with the following command:

$ sudo dpkg -l | grep openssh
ii openssh-client 1:7.6p1-4ubuntu0.1 amd64 secure shell (SSH) client, for secure access to remote machines
ii openssh-server 1:7.6p1-4ubuntu0.1 amd64 secure shell (SSH) server, for secure access from remote machines
ii openssh-sftp-server 1:7.6p1-4ubuntu0.1 amd64 secure shell (SSH) sftp server module, for SFTP access from remote machines

If the "openssh" server package is not installed, this is a finding.

Verify the "sshd.service" is loaded and active with the following command:

Source: https://www.stigviewer.com/stig/canonical_ubuntu_20.04_lts/2022-06-06/finding/V-238215

Advantages / Disadvantages

Advantages

- Validated security guides that are available for a **wide range of products**
- These allow to achieve a **high level of security** (military-grade) and are **free**
- Facilitate Compliance as Code

Disadvantages

- They are very focused on military / certain US departments needs
  - Therefore, some of them may require modifications to adapt them to civilian requirements
- Requires constant monitoring of new versions in case their specifications change
- Its **official SCAP tool** (SCC, SCAP Compliance Checker) that automatize them **is restricted**
  - Only for US government employees and contractors with a `.gov` or `.mil` email address
  - **It is only public for specific systems**
- Therefore, we need to rely in third-party automation implementations of the STIG guides
  - Like the one provided in Ubuntu Pro! (seen later)
  - Or maybe develop our own automation scripts, or use the guidance for **manual checking only**
  - **However, some of them do have public Ansible automated remediation procedures freely available!**

Think you've understood it all? Evaluate yourself!

?

- **You can do the following**
  - *Understand that STIGs are security controls of the U.S. Department of Defense and that many of them are distributed in SCAP format*
  - *Understand that each security control is assigned a security level based on the criticality of the vulnerability that could cause not having them implemented (CAT classification)*
  - *Be clear that the systems to which the controls are applied are classified according to the importance of the information they manage (MAC classification)*
  - *It should also be clear to you that the information managed is also classified according to its confidentiality*
  - *Understand that MAC and confidentiality levels are independent*
  - *Know that many STIGs are free to obtain, and even the official system audit tool (SCC) is available for some OSs as well for free*
  - *Understand the general structure of a STIG safety control*

Center for Internet Security (CIS) Benchmarks

"Top Gun" security controls ☺

*Icons by Bing Chat AI

CIS BENCHMARKS

https://www.cisecurity.org/

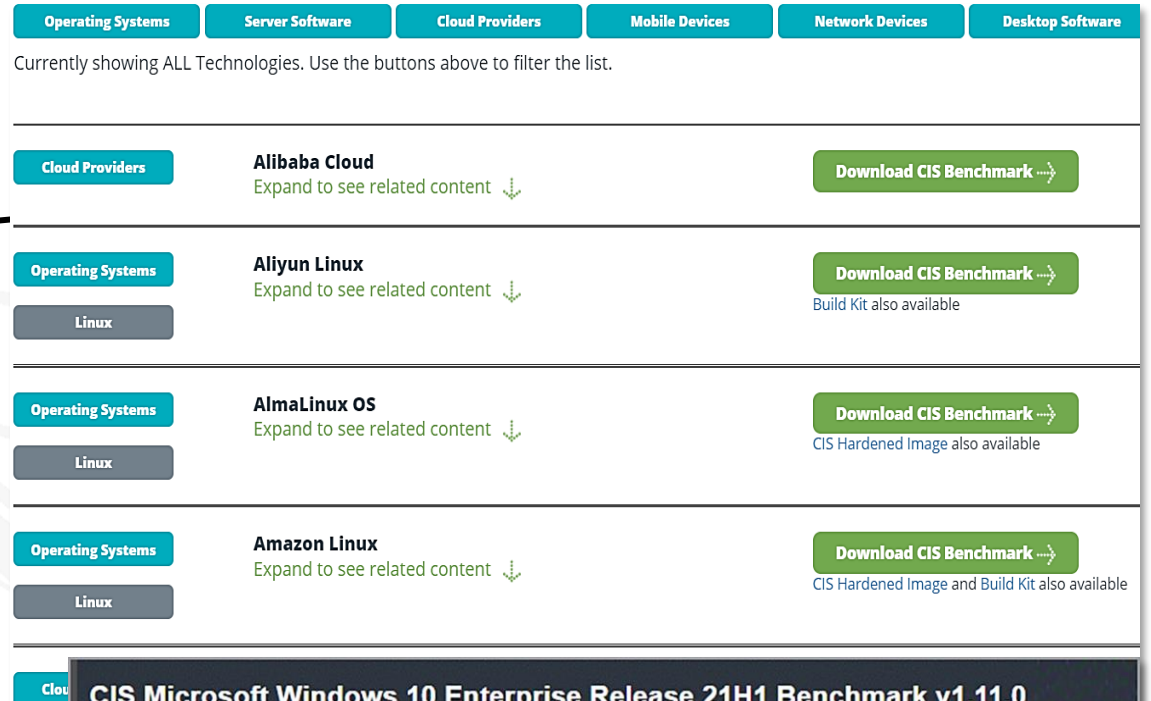
- **Well established source of hardening guides**
  - Recommend values and **technical security controls** applicable to network devices, OS, software...
  - One guide per product and version
  - Currently more than 100 are available: https://www.cisecurity.org/cis-benchmarks/
- **They are created and used by consensus of the US government**
  - Together with 1800 well-known companies from different industries (Adobe, HP,...)
  - Which **guarantees the quality and reliability of their contents**...
  - They contain the most up-to-date knowledge and best security practices
    - From the experience of several major private **civilian companies** and **public institutions** worldwide
- **Apart from guides, they include (not free)**
  - **Prebuilt hardened VMs** on Azure, AWS, Google Cloud
    - https://www.cisecurity.org/cis-hardened-image-list
  - **Build kits** to automate configuration of existing software according to benchmark specifications
    - https://www.cisecurity.org/cis-securesuite/cis-securesuite-build-kit-content

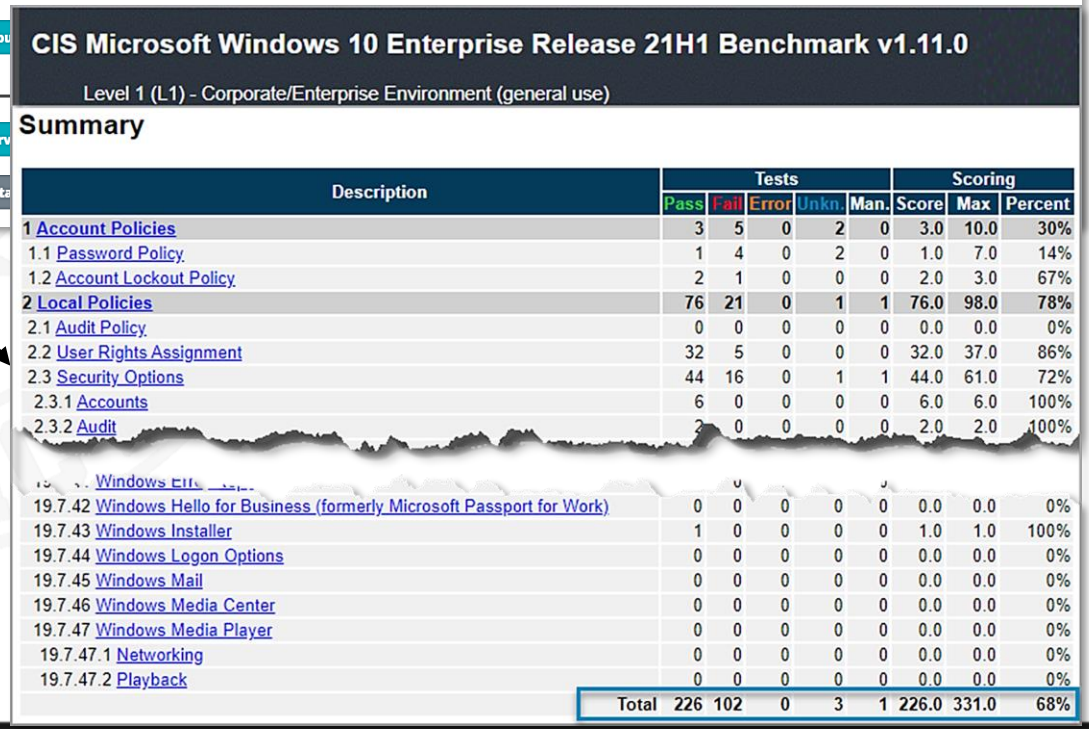
CIS BENCHMARKS

Computer Security

Source: https://www.cisecurity.org/cis-benchmarks/

- **Available in PDF format**
  - **Free, and registration is not required!**
  - https://downloads.cisecurity.org/#/
- **Also available in SCAP formats**
  - With its own SCAP tool (CIS CAT Pro)
  - Free for US educational / authorized institutions, not free for the rest ☹
  - A limited (only 3 benchmarks) **free** version of the tool also exist
    - **CIS-CAT Lite**: https://learn.cisecurity.org/cis-cat-lite
- **SCAP security guide package files also has CIS-based security profiles**
  - **Validate and remediate CIS Benchmarks security controls for a few OS**
  - They are incomplete (several controls are missing)





Why use CIS Benchmarks?

- **Validated by experts**
  - Not a blog, an internet article, a tutorial…or sources whose reliability cannot be checked
- **Complete**
  - There's no missing element to get a certain level of security
- **Fully explained**
  - It tells you **what is wrong**, **how to fix it**, and **why it needs fixing**
- **Updated**
  - Errata are corrected and adapted to new versions of the products (they are **maintained)**
- **International**
  - Complying with these benchmarks enables systems to operate in environments requiring official security certifications or assurances
- **Adapted to the software product**
  - Each benchmark has a **different number of security controls**, and **profiles** that adapt to each product

Security control structure: Automated or manual

- **Systems are evaluated against the security controls of their corresponding CIS benchmarks**
- **Some security controls can be fully automated, others do not**
  - This is indicated on each one
- **Automated**
  - Recommendations for which assessment of a technical control **can be fully automated and validated** to a pass/fail
  - Include the information to **implement automation**
- **Manual**
  - Represents recommendations for which assessment of a technical control cannot be fully automated
  - Requires **all or some manual steps** to validate that the configured state is set as expected
    - The expected state can vary depending on the environment

Source: Ubuntu 22.04 Benchmark PDF file

5.3.3 Ensure sudo log file exists (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

sudo can use a custom log file

Rationale:

A sudo log file simplifies auditing of sudo commands

Impact:

WARNING: Editing the `sudo` configuration incorrectly can cause `sudo` to stop functioning. Always use `visudo` to modify `sudo` configuration files.

Audit:

Run the following command to verify that sudo has a custom log file configured:

```
# grep -rPsi
"^\h*Defaults\h+([^#]+,\h*)?logfile\h*=\h*(\"|\')?\H+(\"|\')?(,\h*\H+\h*)*\h*
(#.*)?$" /etc/sudoers*
```

Verify the output matches:

```
Defaults logfile="/var/log/sudo.log"
```

Remediation:

Edit the file `/etc/sudoers` or a file in `/etc/sudoers.d/` with `visudo` or `visudo -f <PATH TO FILE>` and add the following line:
Example:

```
Defaults logfile="/var/log/sudo.log"
```

References:

1. SUDO(8)
2. VISUDO(8)

Additional Information:

visudo edits the sudoers file in a safe fashion, analogous to vipw(8). visudo locks the sudoers file against multiple simultaneous edits, provides basic sanity checks, and checks for parse errors. If the sudoers file is currently being edited you will receive a message to try again later.

CIS Benchmarks security control structure: Profiles and levels

- Security controls are divided in **usage profiles** and **levels**
- **Usage profiles** depend on what functionality the OS / software is going to fulfill
  - The Ubuntu 18.04 CIS Benchmark defines two usage profiles
    - Server and Workstation
  - The Windows Server 2019 CIS Benchmark also defines two
    - Member Server and Domain controller
- Levels are typically two in all products covered by CIS benchmarks
  - **Level 1**: controls of this level intend to
    - Be practical and not cause unnecessary harm (reasonably keep the functionality of the software)
    - Provide a substantial security advantage
  - **Level 2**: extends level 1 with controls that have the following characteristics
    - Designed for environments or use cases where security is key (**above other things**)
    - Implement an in-depth defense
    - **They could affect the functionality** of the machine or its services in some way, or its performance
  - **Special levels**: some products have special levels defined just for them
    - E. g. Windows Server 2019 has a third level called "Next Generation Windows Security"

CIS Benchmarks security control structure: Profiles and levels

- **Each security control is tagged with the usage profiles in which it is applicable**
  - One, several, or all the defined profiles
- **Examples of tagged security controls**
  - The Ubuntu 18.04 CIS Benchmark has
    - 204 as Level 1 - Server
    - 37 as Level 2 - Server
    - 200 as Level 1 - Workstation
    - 40 as Level 2 - Workstation
  - And the Windows Server 2019 CIS Benchmark has
    - 289 as Level 1 - Domain Controller
    - 60 as Level 2 - Domain Controller
    - 6 as Next Generation Windows Security - Domain Controller
    - 293 as Level 1 - Member Server
    - 61 as Level 2 - Member Server
    - 6 as Next Generation Windows Security - Member Server

5.3.3 Ensure sudo log file exists (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Source: Ubuntu 22.04 Benchmark PDF file

Description:

sudo can use a custom log file

Rationale:

A sudo log file simplifies auditing of sudo commands

Impact:

WARNING: Editing the `sudo` configuration incorrectly can cause `sudo` to stop functioning. Always use `visudo` to modify `sudo` configuration files.

Audit:

Run the following command to verify that sudo has a custom log file configured:

```
# grep -rPsi
"^\h*Defaults\h+([^#]+,\h*)?logfile\h*=\h*(\"|\')?\H+(\"|\')?(,\h*\H+\h*)*\h*
(#.*)?$" /etc/sudoers*
```

Verify the output matches:

```
Defaults logfile="/var/log/sudo.log"
```

Remediation:

Edit the file `/etc/sudoers` or a file in `/etc/sudoers.d/` with `visudo` or `visudo -f <PATH TO FILE>` and add the following line:
Example:

```
Defaults logfile="/var/log/sudo.log"
```

References:

1. SUDO(8)
2. VISUDO(8)

Additional Information:

visudo edits the sudoers file in a safe fashion, analogous to vipw(8). visudo locks the sudoers file against multiple simultaneous edits, provides basic sanity checks, and checks for parse errors. If the sudoers file is currently being edited you will receive a message to try again later.

CIS Benchmarks security control structure: Technical data

- **Description**
  - Details the action
- **Rationale**
  - Describes why it is necessary to do this security control
  - And its impact on the product security
- **Audit**
  - Technical procedure to check whether the security control is currently implemented or not
  - Implemented by **automatic verification** procedures
- **Remediation**
  - How to implement the security control
  - If the audit section returns it is not currently implemented
  - Implemented by **automatic remediation** procedures

Source: Ubuntu 22.04 Benchmark PDF file

5.3.3 Ensure sudo log file exists (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

sudo can use a custom log file

Rationale:

A sudo log file simplifies auditing of sudo commands

Impact:

WARNING: Editing the `sudo` configuration incorrectly can cause `sudo` to stop functioning. Always use `visudo` to modify `sudo` configuration files.

Audit:

Run the following command to verify that sudo has a custom log file configured:

```
# grep -rPsi
"^\h*Defaults\h+([^#]+,\h*)?logfile\h*=\h*(\"|\')?\H+(\"|\')?(,\h*\H+\h*)*\h*
(#.*)?$" /etc/sudoers*
```

Verify the output matches:

```
Defaults logfile="/var/log/sudo.log"
```

Remediation:

Edit the file `/etc/sudoers` or a file in `/etc/sudoers.d/` with `visudo` or `visudo -f <PATH TO FILE>` and add the following line:
Example:

```
Defaults logfile="/var/log/sudo.log"
```

References:

1. SUDO(8)
2. VISUDO(8)

Additional Information:

visudo edits the sudoers file in a safe fashion, analogous to vipw(8). visudo locks the sudoers file against multiple simultaneous edits, provides basic sanity checks, and checks for parse errors. If the sudoers file is currently being edited you will receive a message to try again later.

Advantages / Disadvantages

Advantages

- A comprehensive and detailed guide of technical security controls that turns a system more secure and facilitate **Compliance as Code**
- It tells you precisely what to do, why to do it, and how to do it
- Validated in terms of effectiveness and completeness by 1000s of experts around the world
- Their profiles let you adapt the securing operations to the purpose of each systems

Disadvantages

- Only cover part of the most used products
- The complete SCAP tool is proprietary and not free
  - We can use the free **Lite** version, that only supports **Windows 10**, **Ubuntu**, and **Chrome**
  - https://learn.cisecurity.org/cis-cat-lite
  - https://www.youtube.com/watch?v=76XpFVwdRYg
- We must rely on **unofficial tools or scripts to automate its verification / application** for free
  - Or trust that the `scap-security-guide` support for CIS benchmarks will substantially improve
- Being so extensive, adapting them to a specific functionality can be tedious

OFFICIAL AUTOMATED FREE COMPLIANCE

- **The Ubuntu Pro license turns Ubuntu in an enterprise-grade Linux system**
  - https://ubuntu.com/pro
  - Enables 10 years of package support
  - And gives you access to the Ubuntu Security Guide (`usg` package)
    - Includes **automated compliance with the Ubuntu Pro CIS and DISA STIGs**
      - Defense Information System Agency, from the EEUU Department of Defense (DoD)
    - **CIS**: https://ubuntu.com/security/certifications/docs/usg/cis
    - **DISA STIG**: https://ubuntu.com/security/certifications/docs/disa-stig
  - Requires registration and it is free for up to 5 Ubuntu 18.04LTS+
    - Yes, you can now officially create bullet-proof Ubuntu machines automatically! ☺
    - Using any of the two SCAP sources we saw

- **Microsoft also publishes their own security baselines (security controls to implement) and automation software**
  - Hence, Microsoft has their own standard to do this (neither CIS nor STIG)
  - https://learn.microsoft.com/es-es/windows/security/threat-protection/windows-security-configuration-framework/windows-security-baselines

AUTOMATED COMPLIANCE WITH 3RD-PARTY SCRIPTS OR TOOLS

- **There are tools that have built-in audits with CIS controls**
  - For example, the Wazuh XDR integrates **automated audits** of the OS it monitors
- **These examples uses Ansible to comply with a CIS policy for Ubuntu**
  - **But be careful:** You must be very confident that its content is correct and without "surprises“ ☹
  - https://medium.com/@cosmin.ciobanu/the-quest-for-os-hardening-8affa979f36a
  - https://github.com/florianutz/Ubuntu1804-CIS
  - https://github.com/florianutz/ubuntu2004_cis
- **There are STIGs and CIS Benchmarks available for Windows systems**
  - Both client (Windows 10, 11) and server versions
  - Bash remediation is replaced by PowerShell remediation
  - Ansible cannot be directly installed in Windows, but a Windows machine can be configured from a remote Linux one if we have appropriate permissions
    - Our student María Flórez implemented this as her final degree project
    - https://github.com/Yori1999/vagrant-ansible-hardening
  - We also have the Hardening Kitty scripts: https://github.com/scipag/HardeningKitty

➢ Exercise **L6B4_CISWAZUH**

Think you've understood it all? Evaluate yourself!

?

- **You can do the following**
  - *Understand what CIS Benchmarks are, who maintains them, and where they can be downloaded from*
  - *Understand the meaning of a security check classified as automated versus one classified as manual*
  - *Understand what usage profiles are and what they depend on each system*
  - *Understanding the difference between a Level 1 and Level 2 CIS Control*
  - *Understand what information you can find in the description, rationale, audit, and remediation sections of each control*
  - *Be clear about what the Ubuntu Pro license offers regarding CIS (and STIGs)*
  - *And also, that there are ways to achieve CIS compliance with third-party tools, but understanding the risks involved*

< Go to Index

SECURITY FRAMEWORKS

Using technical security controls to create security policies and achieving a higher abstraction level

*Icons by Bing Chat AI

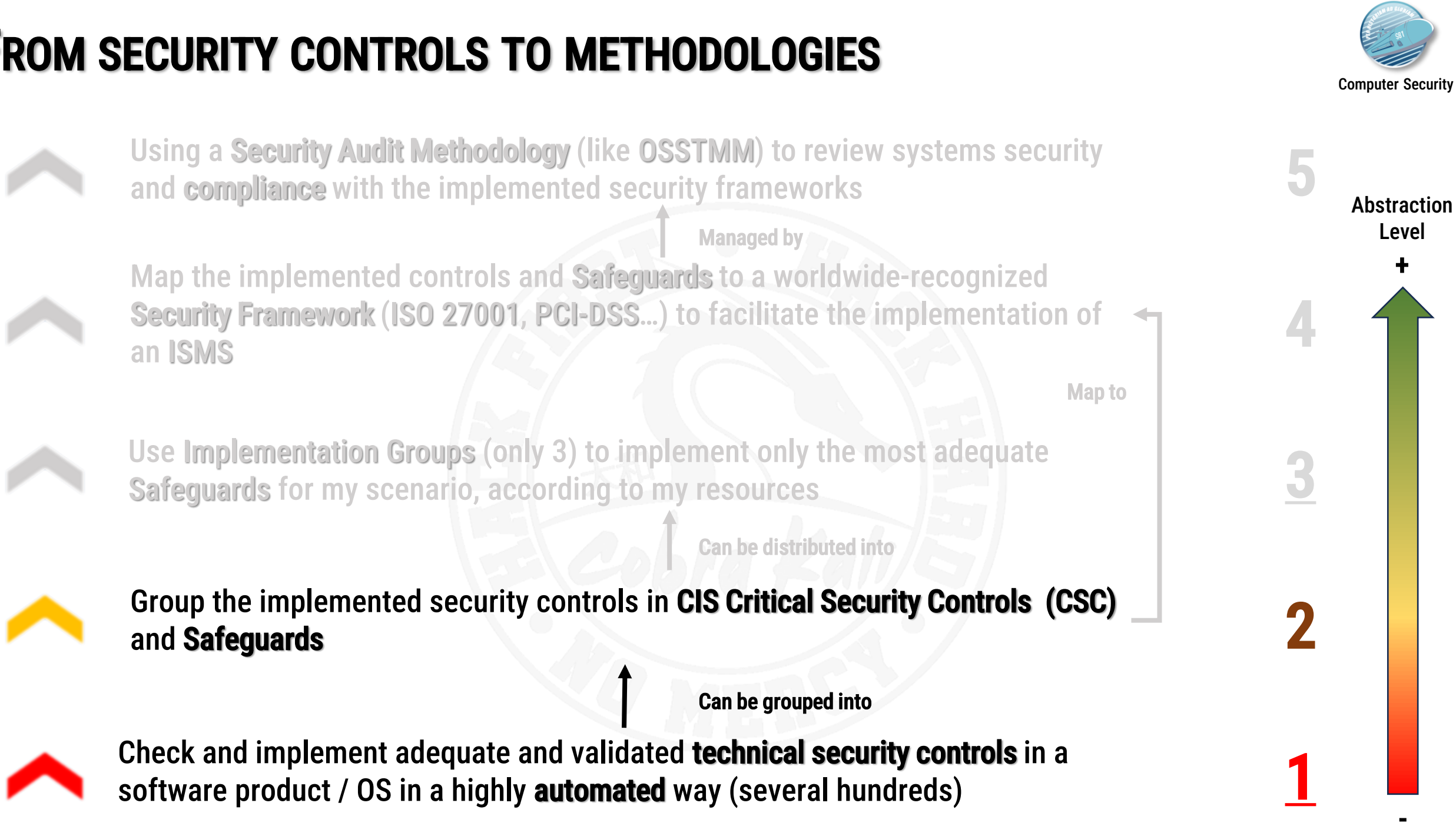
Source: Bing Chat AI

Departamento de Informática
Universidad de Oviedo

What are you going to find in this block?

- **In this block you will learn**
  - Understand what **CSC security controls** are, and how they relate to CIS Benchmarks
  - How you can **implement CSC controls** based on implementing CIS Benchmarks technical security controls
  - What **Implementation Groups** are, and what they mean
  - How to use the implementation of CSC controls to later facilitate **compliance** with different security standards

From security controls to methodologies



Beyond security control technical guidelines

- **Applying hundreds of validated security controls ensures a proper security level**
  - But they are difficult to handle when security is implemented in an infrastructure (too many!)
- **We need higher level abstractions that group the security controls in fewer entities**
  - We need to identify **what kind of hardening** have been performed on each system more easily
    - This is key to implement security frameworks and facilitate security audits
  - On a **higher abstraction level**, we need things like "*passwords must meet a high security standard*"
    - Not low-level technical actions like the ones in the security controls. E. g.:
      - To install and configure the Linux `libpam` package
      - Assign the values X, Y, Z to certain entries of a Windows Domain Controller security policy
  - Therefore, we need something that **isolate us from the technical details** of each system
    - Focusing on "**what**" instead of "how" (**detailed technical information does not belong to this level**!)
    - These "what" abstractions should group hundreds of "how" security controls **in fewer entities**
- **CIS benchmarks allows you to attain a higher abstraction level**
  - Starting from the implemented technical security controls we previously described

CIS Critical Security Controls (CSC controls) v8

- They are an organized set of Safeguards
  - Also called CSC Controls or CIS Controls
- They were designed to mitigate the main system and network attacks
- They can be mapped to and are referred by multiple security, management, and legal frameworks
- Version v8 has been designed to deal with the newest threats
  - Cloud, virtualization, remote work attacks, new attack tactics…

General organization of the CSC Controls v8 and its Safeguards:
https://www.linkedin.com/pulse/cis-critical-security-controls-v8-steps-template-download-dan-duran/

CIS Critical Security Controls (CSC controls) v8

- **At the end of each technical security control of any CIS benchmark we can find which CSC Controls and Safeguards are associated with it**
  - CSC Controls represent **18** (**v8**) or **20** (**v7**) recognized best defensive cybersecurity practices
  - They are subdivided in **153 Safeguards (v8)** (or **170 CSC subcontrols (v7)**)
- ***What does this table mean?***
  - That this technical security control belongs to the **CSC Control v8 nº 3** "*Data Protection*"
    - See the previous table
  - Inside it, it belongs to the **Safeguard 3.3** "*Configure Data Access Control Lists*"

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

- **If we have used the v71, this image means that this technical security control belongs to the CSC Control v7 number 14 "Controlled Access Based on Net to Know"**
- **Inside it, it is also applicable to the CSC Subcontrol 14.6 of that CSC control 14**
- **The version 7.1 will be superseded by the v8**

CIS Critical Security Controls (CSC controls) v8

- **The CSC Controls…**
  - Are developed by **consensus**, containing **expert information** about cybernetic threats & technologies
  - Model different types of actions: from basic cybersecurity operations to very advanced ones
  - Are used to quickly set protections that could benefit any company
- **The 18 CSC Controls v8 and their associated 153 Safeguards are always the same**
  - No matter the software product / OS
  - They were designed to cover the security considerations of **ALL** software / OS that could have a CIS Benchmark
- **But each CIS Benchmark only contain reasonable Safeguards for their software**
  - E. g. The Google Chrome CIS Benchmark explains how to harden this browser
    - It does not have any technical security control mapping to any Safeguard of the CSC Control 1 "*Inventory and Control of Hardware Assets*"
    - It is a browser, not infrastructure!
  - This means that the software **does not have to implement all the 153 Safeguards**, but much less!
  - So 100s of technical security controls are grouped in just 10s entities

From technical security controls to CSC Controls

Ubuntu 22.04
CIS Benchmark (PDF)

CSC Controls v8
(and its Safeguards)

https://www.cisecurity.org/controls/cis-controls-navigator

All technical security controls belonging to Safeguard 3.3

CSC Control 3 – *Data Protection*

- ***Safeguard 3.3***: *Configure Data Access Control Lists*

All technical security controls belonging to Safeguards 4.3 and 4.8

CSC Control 4 – *Secure Configuration of Enterprise Assets and Software*

- ***Safeguard 4.3***: *Configure Automatic Session Locking on Enterprise Assets*
- ***Safeguard 4.8***: *Uninstall or Disable Unnecessary Services on Enterprise Assets and Software*

All technical security controls belonging to Safeguards 8.2 and 8.9

CSC Control 8 – *Audit Log Management*

- ***Safeguard 8.2***: *Collect Audit Logs*
- ***Safeguard 8.9***: *Centralize Audit Logs*

CIS Control 3 - Data Protection

- Safeguard 3.1: Establish and Maintain a Data Management Process
- Safeguard 3.2: Establish and Maintain a Data Inventory
- Safeguard 3.3: Configure Data Access Control Lists
- Safeguard 3.4: Enforce Data Retention

CIS Control 4 - Secure Configuration of Enterprise Assets and Software

- Safeguard 4.1: Establish and Maintain a Secure Configuration Process
- Safeguard 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure
- Safeguard 4.3: Configure Automatic Session Locking on Enterprise Assets
- Safeguard 4.4: Implement and Manage a Firewall on Servers
- Safeguard 4.5: Implement and Manage a Firewall on End-User Devices
- Safeguard 4.6: Securely Manage Enterprise Assets and Software
- Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software
- Safeguard 4.8: Uninstall or Disable Unnecessary Services on Enterprise Assets and Software

CIS Control 8 - Audit Log Management

- Safeguard 8.1: Establish and Maintain an Audit Log Management Process
- Safeguard 8.2: Collect Audit Logs
- Safeguard 8.3: Ensure Adequate Audit Log Storage
- Safeguard 8.4: Standardize Time Synchronization
- Safeguard 8.5: Collect Detailed Audit Logs
- Safeguard 8.6: Collect DNS Query Audit Logs
- Safeguard 8.7: Collect URL Request Audit Logs
- Safeguard 8.8: Collect Command-Line Audit Logs
- Safeguard 8.9: Centralize Audit Logs
- Safeguard 8.10: Retain Audit Logs

FROM SECURITY CONTROLS TO METHODOLOGIES

Computer Security

Using a **Security Audit Methodology** (like **OSSTMM**) to review systems security and **compliance** with the implemented security frameworks

5

Managed by

Map the implemented controls and **Safeguards** to a worldwide-recognized **Security Framework** (**ISO 27001, PCI-DSS…**) to facilitate the implementation of an **ISMS**

4

Map to

Use **Implementation Groups** (only 3) to implement only the most adequate **Safeguards** for my scenario, according to my resources

3

Can be distributed into

Group the implemented security controls in **CIS Critical Security Controls (CSC)** and **Safeguards**

2

Can be grouped into

Check and implement adequate and validated **technical security controls** in a software product / OS in a highly **automated** way (several hundreds)

1

Abstraction Level

+

-

Implementation groups (IGs)

- In a previous slide about CSC Controls, you saw this… *What is an IG?*
- CSC Controls are used by companies that worry about and invest in cybersecurity
  - With widely different risk exposures
  - And to set up an efficient cybersecurity policy
- However, in some scenarios applying CSC Controls is difficult
  - Especially when the security budget is limited
- This is the reason why IGs (**Implementation Groups**) were created

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

Implementation groups (IGs)

- IGs provide
  - A new **classification / prioritization** of the Safeguards of each CSC Control
  - A **methodology** to improve the evaluation of the security level of the company resources
- **Companies evaluate themselves and chose one IG**
  - Now they have only to focus to fulfill all the Safeguards belonging to that IG
- **In other words: it narrows down how many Safeguards you must implement**
  - But considering the company **perceived security risks** and its **economic resources**
  - As you saw, all Safeguards of the technical security controls are mapped to one or more IG
  - Therefore, IGs **filter what technical actions you must implement on your systems**
  - **Only those that have been included in the Safeguards of the IG you choose!**
    - In the previous table, that technical security control must be implemented, no matter the IG you chose
    - It belongs to all of them!

3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●

Implementation groups (IGs)

- **So, IGs are categories that companies may use to auto-evaluate their security**
  - Based on the cybersecurity attributes they consider relevant in their use case
  - So, each IG identifies what Safeguards (and CSC Controls) are reasonable for companies with a certain risk profile and number of economic resources to implement security operations
    - This way, any company can classify itself into one IG and focus their economic resources to improve security using **only** the CSC Subcontrols included in that IG
- **Each IG includes the previous one, and there are three**
  - **IG1**: a basic set of CSC Subcontrols to implement by companies with a limited risk exposure, experience, and resources to invest in cybersecurity
    - **It is the "cyber-hygiene" level**: essential protections that must be established to defend against attacks
    - **Every company should implement at least an IG1 level**
  - **IG2**: additional Safeguards to be implemented by companies with more resources and experience
    - But also with a higher risk exposure than IG1 companies
  - **IG3**: incorporates the rest of CSC Subcontrols not included in the previous levels
    - **Maximum risk exposure** and hence economical cost, but also the maximum security level

IMPLEMENTATION GROUPS (IGS)

Computer Security

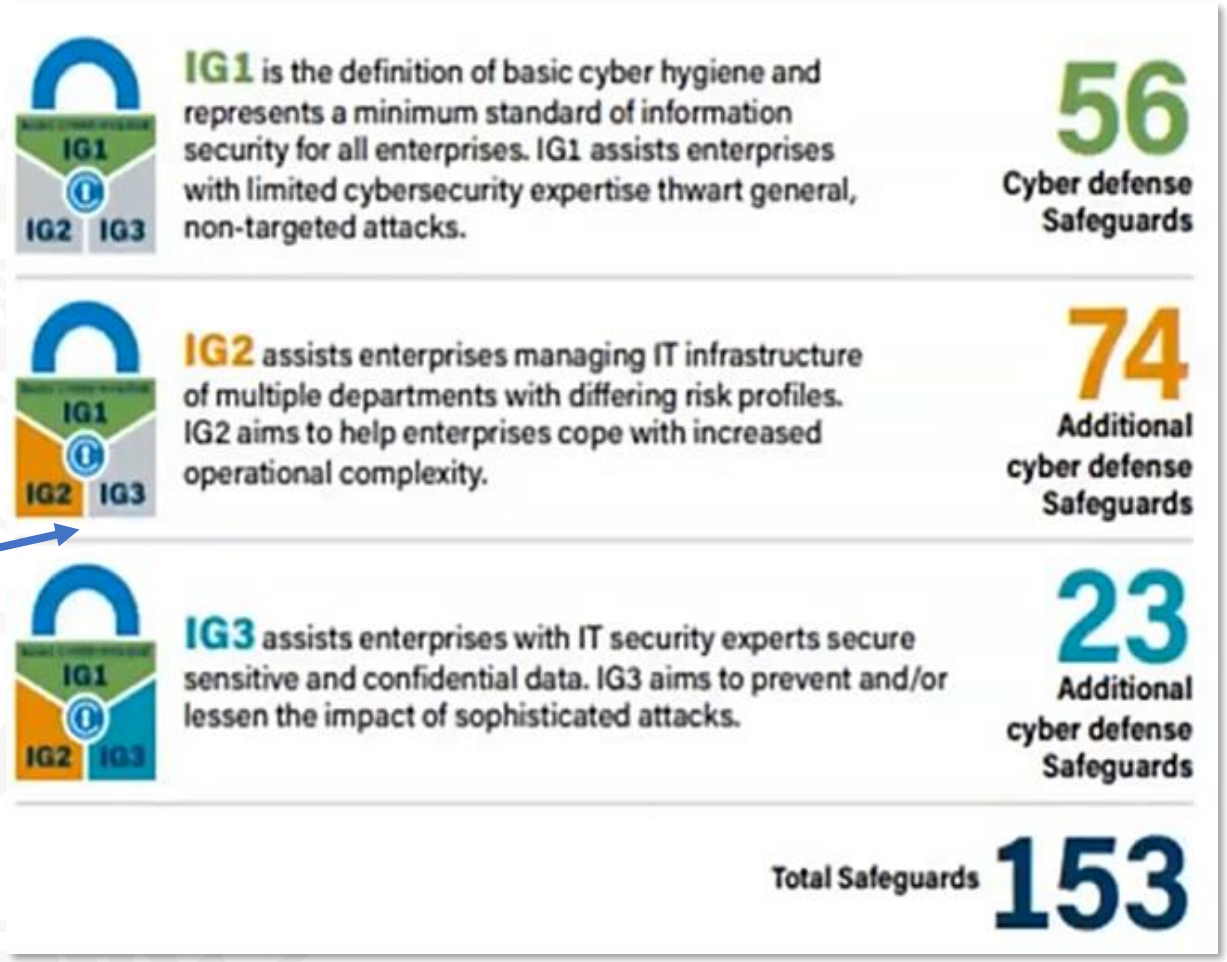
Source: https://www.itpromentor.com/cisv8-assessment-tool/

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●

Which IGs does this security control belong to

From the 14 Safeguards of the CSC Control 3 "*Data Protection*", 6 belong to IG1, 6 more (12 in total) to IG2, and all 14 to IG3



E. g.: I'm a small shop that sells a limited catalog of clothes on Internet. All my payments are managed by PayPal, and user authentication relies on Google, so I don't really store very critical data.
I will classify myself as IG1, so now I will follow only the Safeguards of this Implementation Group, and implement all the related technical security controls of the CIS Benchmark of my Ubuntu 22.04 + Apache 2 web server that are related to them

CIS, SECURITY FRAMEWORKS, AND POLICIES

- **IGs focus the cybersecurity efforts of a company in the most important areas**
  - Maximizes resource usage considering their risk
- **However, it is a CIS methodology**
  - We may need something that follows international security standards and frameworks
  - We need **worldwide-accepted management procedures**
- **When companies seriously invest in cybersecurity, they need to implement security frameworks**
  - **But this does not mean that we wasted our time using the CIS Benchmarks as technical guidelines!**
  - Quite the contrary, lots of popular security frameworks mention or use them
  - https://www.cisecurity.org/cybersecurity-tools/mapping-compliance/
- **Multiple security frameworks are used worldwide, some applied on certain sectors**
  - CIS Benchmarks **may help us to achieve compliance with lots of them**
  - The following slide show some of them

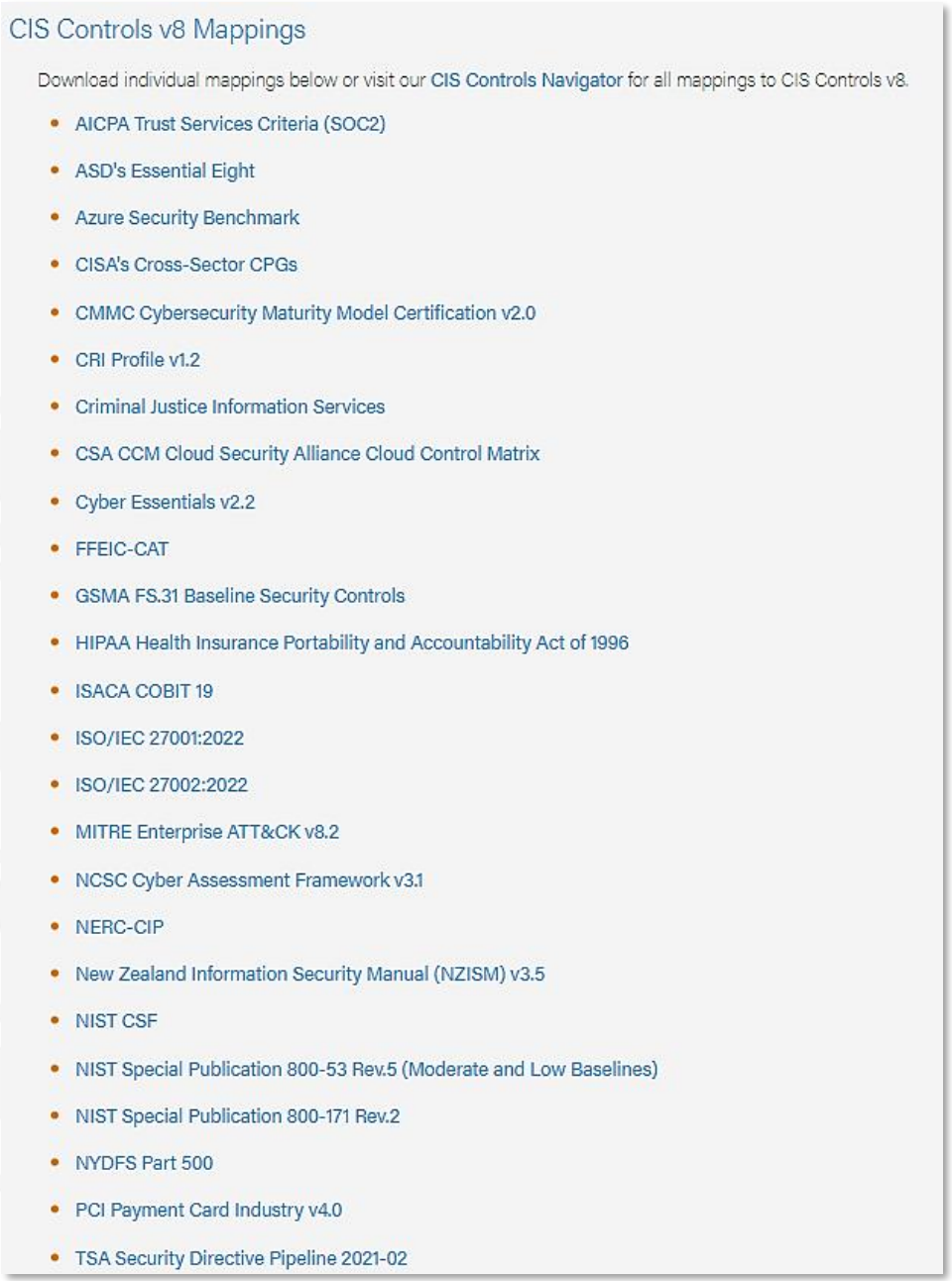
CIS, SECURITY FRAMEWORKS, AND POLICIES

- **Payment Card Industry Data Security Standard (PCI DSS)**
  - Used by some of the **major retailers** in the world
  - Mentions CIS Benchmarks as a recommended hardening standard to facilitate its compliance
- **National Institute of Standards and Technology (NIST) and Federal Information Security Modernization Act (FISMA)**
  - NIST is a **leader agency in technical compliance**; FISMA is a part of NIST
  - CIS controls greatly facilitate to achieve compliance with NIST security standards
  - The National Checklist Program Repository recommends CIS Benchmarks to federal agencies and companies that try to achieve compliance with FISMA standards
- **Health Insurance Portability and Accountability Act (HIPAA)**
  - Security baselines to protect **patient data on health-related companies**/organizations
  - CIS controls have lots of common characteristics with HIPAA; they can be a complement
  - They are also a way to enable health-related companies/organizations to better respond to the latest attack techniques

CIS, SECURITY FRAMEWORKS, AND POLICIES

Computer Security

- **General Data Protection Regulation** 2016/679 of the European Union (**ASLEPI**)
  - https://www.cisecurity.org/gdpr/
- **International Organization for Standardization** (ISO) ISO/IEC 27001 (next section)
  - Provides **independent and validated worldwide standards to ensure cybersecurity**
  - It helps companies to defend against cybernetic threats and security risks
- There are **STIGs <-> CIS Benchmarks** mappings
  - https://www.cisecurity.org/blog/new-options-from-cis-for-stig-compliance/
- There are no **ENS <-> CIS Benchmarks** mappings
  - Although both can be mapped to ISO 27001, so this can be used as a "bridge" between both


CIS Controls v8 Mappings

Download individual mappings below or visit our CIS Controls Navigator for all mappings to CIS Controls v8.

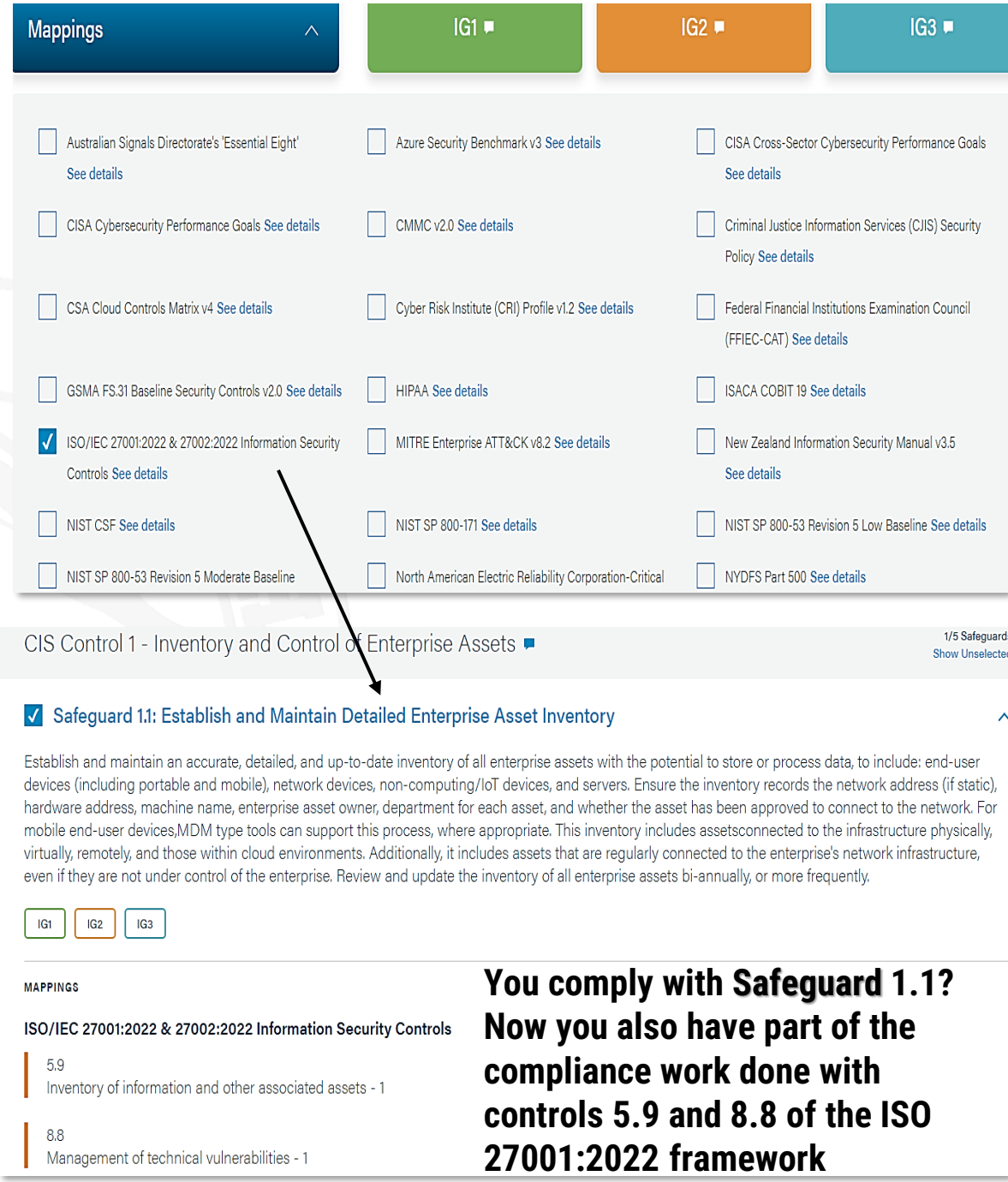
- AICPA Trust Services Criteria (SOC2)
- ASD's Essential Eight
- Azure Security Benchmark
- CISA's Cross-Sector CPGs
- CMMC Cybersecurity Maturity Model Certification v2.0
- CRI Profile v1.2
- Criminal Justice Information Services
- CSA CCM Cloud Security Alliance Cloud Control Matrix
- Cyber Essentials v2.2
- FFEIC-CAT
- GSMA FS.31 Baseline Security Controls
- HIPAA Health Insurance Portability and Accountability Act of 1996
- ISACA COBIT 19
- ISO/IEC 27001:2022
- ISO/IEC 27002:2022
- MITRE Enterprise ATT&CK v8.2
- NCSC Cyber Assessment Framework v3.1
- NERC-CIP
- New Zealand Information Security Manual (NZISM) v3.5
- NIST CSF
- NIST Special Publication 800-53 Rev.5 (Moderate and Low Baselines)
- NIST Special Publication 800-171 Rev.2
- NYDFS Part 500
- PCI Payment Card Industry v4.0
- TSA Security Directive Pipeline 2021-02

Mappings from the CSC Controls v8 to other frameworks: https://www.cisecurity.org/controls/v8

From CIS CSC controls to security frameworks

Computer Security

- **CIS way to help to complying with multiple frameworks is documented**
  - CSC controls and Safeguards can be mapped to elements used by other frameworks
    - https://www.cisecurity.org/controls/cis-controls-navigator/
- **This way**
  - CIS benchmarks technical controls ensure proper hardening of any software
  - Once implemented, you can calculate how many CSC Controls and Safeguards you are covering
  - Then, you can **map** them to a cybersecurity framework you must implement
    - This way, your technical work can be translated to any of those frameworks
  - So, you can now implement an ISMS easier
    - See next section



You comply with Safeguard 1.1? Now you also have part of the compliance work done with controls 5.9 and 8.8 of the ISO 27001:2022 framework

THINK YOU'VE UNDERSTOOD IT ALL? EVALUATE YOURSELF!

?

- **You can do the following**
  - *Understand that CSC controls are always the same for any software, and that they are one more level of abstraction than technical controls such as **CIS Benchmarks***
  - *Be aware of where you can find the relationship of a technical control with its associated CSC control*
  - *Understand the relationship between CIS technical controls and **Safeguards***
  - *Understand the concept of **Safeguard** and its relationship to **CSC Controls***
  - *You know what each **Implementation Group** is, what they mean, how they are used, and who chooses which one each organization that applies them to is in*
    - *Including its relationship with CSC Controls Safeguards*
  - *You understand how it is possible to move from CIS technical security controls to Safeguards, from there to CSC Controls and, thanks to the latter, be able to partially implement the controls of many security frameworks used today*
    - *Thus, understanding that all the work done on the console (manual or automated) can be used at higher levels of abstraction*

< Go to Index

How to implement >

ISMS IMPLEMENTATION

What is an Information Security Management System?

*Icons by Bing Chat AI

Source: Bing Chat AI

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo

What are you going to find in this block?

- **In this block you will learn**
  - What exactly an **ISMS** is, and the benefits of implementing one
  - What it means to **implement an ISMS** and its security controls
  - That there are several security standards, and that ISO 27000 is an internationally recognized one
  - And about the **ISO 27000:2022 standard** specifically...
    - What the 27001 and 27002 standards are, and how do they relate to each other
    - What the structure of an ISO 27002:2022 security control is

From security controls to methodologies

Computer Security

Using a **Security Audit Methodology** (like **OSSTMM**) to review systems security and **compliance** with the implemented security frameworks

5

Managed by

Map the implemented controls and **Safeguards** to a worldwide-recognized **Security Framework** (ISO 27001, PCI-DSS…) to facilitate the implementation of an **ISMS**

4

Map to

Use **Implementation Groups** (only 3) to implement only the most adequate **Safeguards** for my scenario, according to my resources

3

Can be distributed into

Group the implemented security controls in **CIS Critical Security Controls (CSC)** and **Safeguards**

2

Can be grouped into

Check and implement adequate and validated **technical security controls** in a software product / OS in a highly **automated** way (several hundreds)

1

Abstraction Level

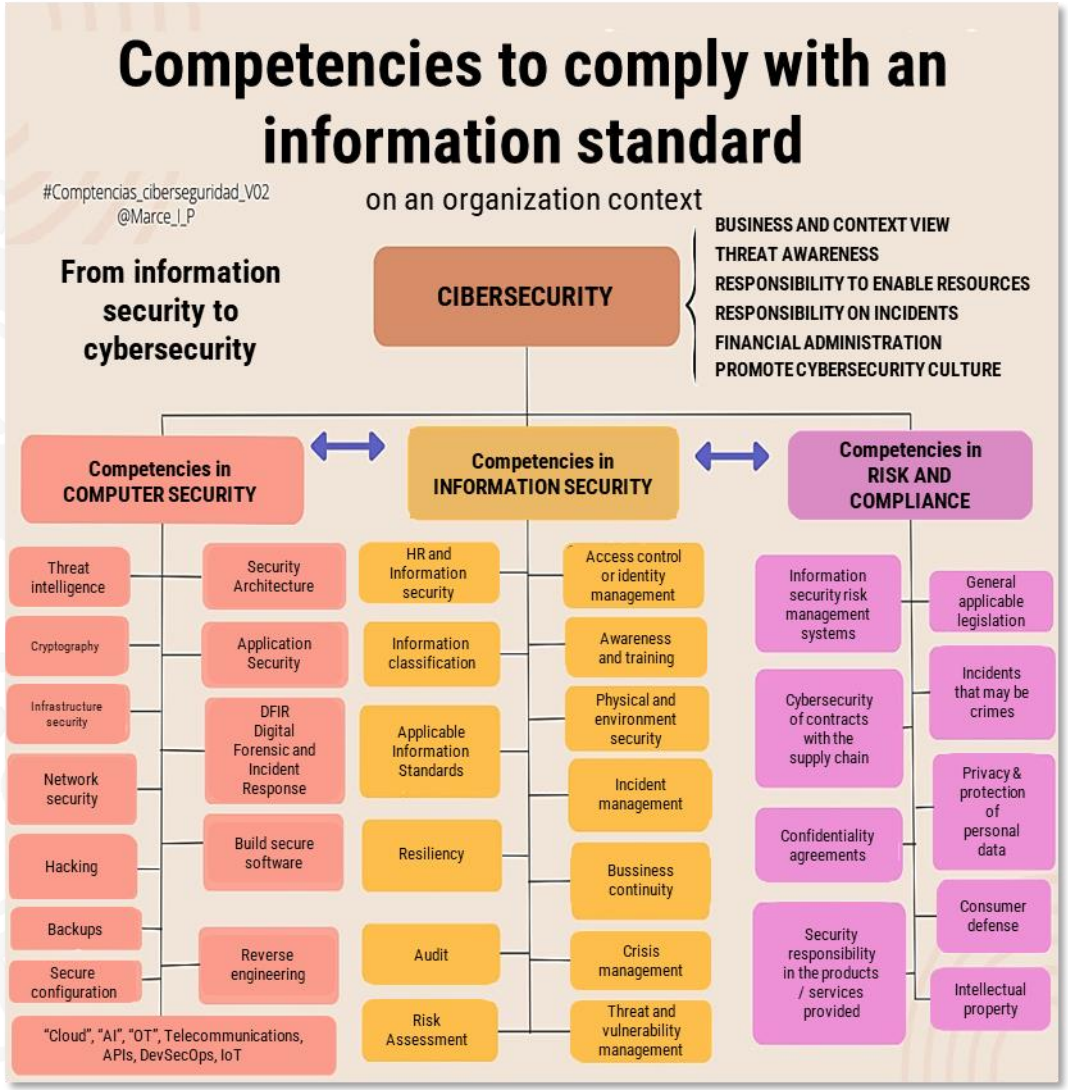
+

-

Information Security Management System (ISMS)

- **Security management must be done**
  - Through a **systematic**, **documented** and **known** process
  - **Fully accepted** company-wide (no exclusions, no matter experience, position…)
- **This process is called Information Security Management System** (ISMS)
- **Its goal is**

  *"Guarantee that information security **risks** are **known**, **assumed**, **managed** and **minimized** by a company using a documented, systematic, structured, repeatable, efficient procedure, that must also be adapted to respond **to risk, environment and technology changes**"*
- **Full guarantee is NEVER possible**
  - But ensures that a company is ready to assume loss of CIA of its information



Competences that any ISMS implementation standard must have

ISMS ELEMENTS

- A **security policy**, **organization structure**, **procedures**, **processes** and **resources** are needed for its implementation
- Deploying one means that a company
  - **Studied** the potential risks that their information may suffer
  - **Evaluated** its risk level
  - **Implemented** technologic and organizational **security controls**
    - For those risks that are beyond this risk level
  - **Documented** related policies and procedures
  - Deployed a continuous **review and improvement** process of the whole system
- ISMS are implemented through standards that guarantee the properties of the previous image, such as
  - The **ITIL framework** (Information Technology Infrastructure Library, mentioned in DPPI)
  - The **COBIT framework** (Control Objectives for Information and Related Technologies):
    - https://www.isaca.org/resources/cobit
  - The **ISO 27000 family of standard** (reviewed in the next section)

ISMS IMPLEMENTATION STANDARDS

- **There are many standards, and implementing one or the other depends on the context**
  - Objectives to be achieved
  - Country in which the company is located
    - E.g.: In the U.S., it is very likely that NIST standards will be required
  - The certifications requested by our potential clients
- **The advantage of ISO 27000 is that it is for international adoption**

COBIT	ISO 27001	NIST
Control Objectives for Information and Related Technologies	**International Organization for Standardization**	**National Institute of Standards and Technology**
It's a framework developed by ISACA that focuses on governance and management of information & technology. It provides a set of control objectives to help organizations achieve their business objectives through effective management and governance of their IT assets.	It's a global standard for Information Security Management Systems (ISMS). It outlines the criteria for establishing, implementing, maintaining, and continually improving an information security management system. The standard includes a set of controls that organizations can implement to manage information security risks.	The NIST Cybersecurity Framework provides a set of guidelines and best practices for organizations to manage and improve their ability to prevent, detect, respond to, and recover from cybersecurity events. It is widely used in the United States and has been adopted globally.
FOCUS : Business and IT Governance. Emphasizes information governance and process improvement	**FOCUS :** Information security systems. Systematic approach to managing sensitive company information	**FOCUS :** Cybersecurity and Risk Management. Emphasizes continuous monitoring and risk assessment
PURPOSE : Aligning business goals with IT functions and ensuring effective risk management	**PURPOSE :** Establishing, implementing, maintaining, and improving an information security management system	**PURPOSE :** Providing a flexible and comprehensive approach to managing and mitigating cybersecurity risk
APPLICABILITY : Broad spectrum, suitable for all organization sizes	**APPLICABILITY :** Globally recognized, suitable for any organization	**APPLICABILITY :** Widely used in the United States, adopted globally
KEY FUNCTIONS : Control objectives, Risk management, Information governance, Process improvement, IT alignment	**KEY FUNCTIONS :** Risk assessment, Security policy, Access control, Cryptography, Incident response, Continual improvement	**KEY FUNCTIONS :** Identify, Protect, Detect, Respond, Recover, Continuous monitoring

ISMS DEPLOYMENT ADVANTAGES

- **Reduce the risks,** following their monitoring controls
  - Threats are reduced; damage, if any, is minimized
- **Cost savings** due to resource usage optimization
  - Risk estimation reduces unnecessary and inefficient investments
- Company security has a **methodical and controlled life cycle** in which the entire organization participates
- Compliance with the **legal framework** that protects the organization (**ASLEPI**)
  - https://www.agpd.es/portalwebAGPD/canalresponsable/obligaciones/medidas_seguridad/index-ides-idphp.php
  - http://administracionelectronica.gob.es/ctt/ens
- **Improves market competitivity**: public administrations usually require security certifications to companies
  - When they want to compete for contracts/resources related to information systems
  - In Spain, the CCN CERT forces compliance with the ENS to the software of the public administrations

The international ISO 27001:2022/27002:2022 standard

An international framework to implement an ISMS

*Official icon of the ISO organization

ISO (International Organization for Standardization) / IEC (International Electrotechnical Commission) 27000

- Provides an **Information Security Management framework** for any organization composed by several standards, such as the **ISO/IEC 27001** and **27002**
  - Contains the requirements for establishing, implementing, operating, monitoring, maintaining, and improving an ISMS
  - The only standard in the 27000 family that is **certifiable** once it is implemented **is the 27001**
  - The 27001 is a **management standard** that collects
    - System **components**
    - The **minimum documents** that are part of it
    - The **records** (logs)
    - The security controls to be implemented (up to 93, listed **in the Annex A of the standard**)
      - It contains a basic general view of the security controls needed for implementing an ISMS
  - The **security measures customized** to the needs of each organization
- AENOR is the main Spanish certification agency
  - Asociación Española de NORmalización y certificación: http://www.aenor.es/aenor/inicio/home/home.asp

ANNEX A OF THE 27001:2022 STANDARD

Computer Security

- **Divides its 93 security controls in 4 chapters**
  - **Organizational** controls (37)
  - **People** controls(8)
  - **Physical** controls(14)
  - **Technological** controls(34)
- **Evolution of the 27001:2013**
  - **Detailed description** (free):
    - https://normaiso27001.es/
  - **More information**
    - https://www.escuelaeuropeaexcelencia.com/2022/11/publicada-la-nueva-iso-270012022-novedades-del-estandar-de-seguridad-de-la-informacion/
    - https://blog.innevo.com/iso27001-2022

ISO 27001 and ISO 27002. Information security controls, 2022

5. Organizational controls	6. People controls	8. Technological controls
5.1. Policies for information security	6.1. Screening	8.1. User endpoint devices
5.2. Information security roles and responsibilities	6.2. Terms and conditions of employment	8.2. Privileged access rights
5.3. Segregation of duties	6.3. Information security awareness, education and training	8.3. Information access restriction
5.4. Management responsibilities	6.4. Disciplinary process	8.4. Access to source code
5.5. Contact with authorities	6.5. Responsibilities after termination or change of employment	8.5. Secure authentication
5.6. Contact with special interest groups	6.6. Confidentiality or non-disclosure agreements	8.6. Capacity management
5.7. Threat intelligence	6.7. Remote working	8.7. Protection against malware
5.8. Information security in project management	6.8. Information security event reporting	8.8. Management of technical vulnerabilities
5.9. Inventory of information and other associated assets	**7. Physical controls**	8.9. Configuration management
5.10. Acceptable use of information and other associated assets	7.1. Physical security perimeter	8.10. Information deletion
5.11. Return of assets	7.2. Physical entry	8.11. Data masking
5.12. Classification of information	7.3. Securing offices, rooms and facilities	8.12. Data leakage prevention
5.13. Labelling of information	7.4. Physical security monitoring	8.13. Information backup
5.14. Information transfer	7.5. Protecting against physical and environmental threats	8.14. Redundancy of information processing facilities
5.15. Access control	7.6. Working in secure areas	8.15. Logging
5.16. Identity management	7.7. Clear desk and clear screen	8.16. Monitoring activities
5.17. Authentication information	7.8. Equipment siting and protection	8.17. Clock synchronization
5.18. Access rights	7.9. Security of assets off-premises	8.18. Use of privileged utility programs
5.19. Information security in supplier relationships	7.10. Storage media	8.19. Installation of software on operational systems
5.20. Addressing information security within supplier agreements	7.11. Supporting utilities	8.20. Network security
5.21. Managing information security in the ICT supply chain	7.12. Cabling security	8.21. Security of network services
5.22. Monitoring, review and change management of supplier services	7.13. Equipment maintenance	8.22. Segregation of networks
5.23. Information security for use of cloud services	7.14. Secure disposal or re-use of equipment	8.23. Web filtering
5.24. Information security incident management planning and preparation		8.24. Use of cryptography
5.25. Assessment and decision on information security events		8.25. Secure development life cycle
5.26. Response to information security incidents		8.26. Application security requirements
5.27. Learning from information security incidents		8.27. Secure system architecture and engineering principles
5.28. Collection of evidence		8.28. Secure coding
5.29. Information security during disruption		8.29. Security testing in development and acceptance
5.30. ICT readiness for business continuity		8.30. Outsourced development
5.31. Legal, statutory, regulatory and contractual requirements		8.31. Separation of development, test and production environments
5.32. Intellectual property rights		8.32. Change management
5.33. Protection of records		8.33. Test information
5.34. Privacy and protection of PII		8.34. Protection of information systems during audit testing
5.35. Independent review of information security		
5.36. Compliance with policies, rules and standards for information security		
5.37. Documented operating procedures		

*New control, 2022

by Andrey Prozorov, CISM, CIPP/E, CDPSE, LA 27001 - www.patreon.com/AndreyProzorov

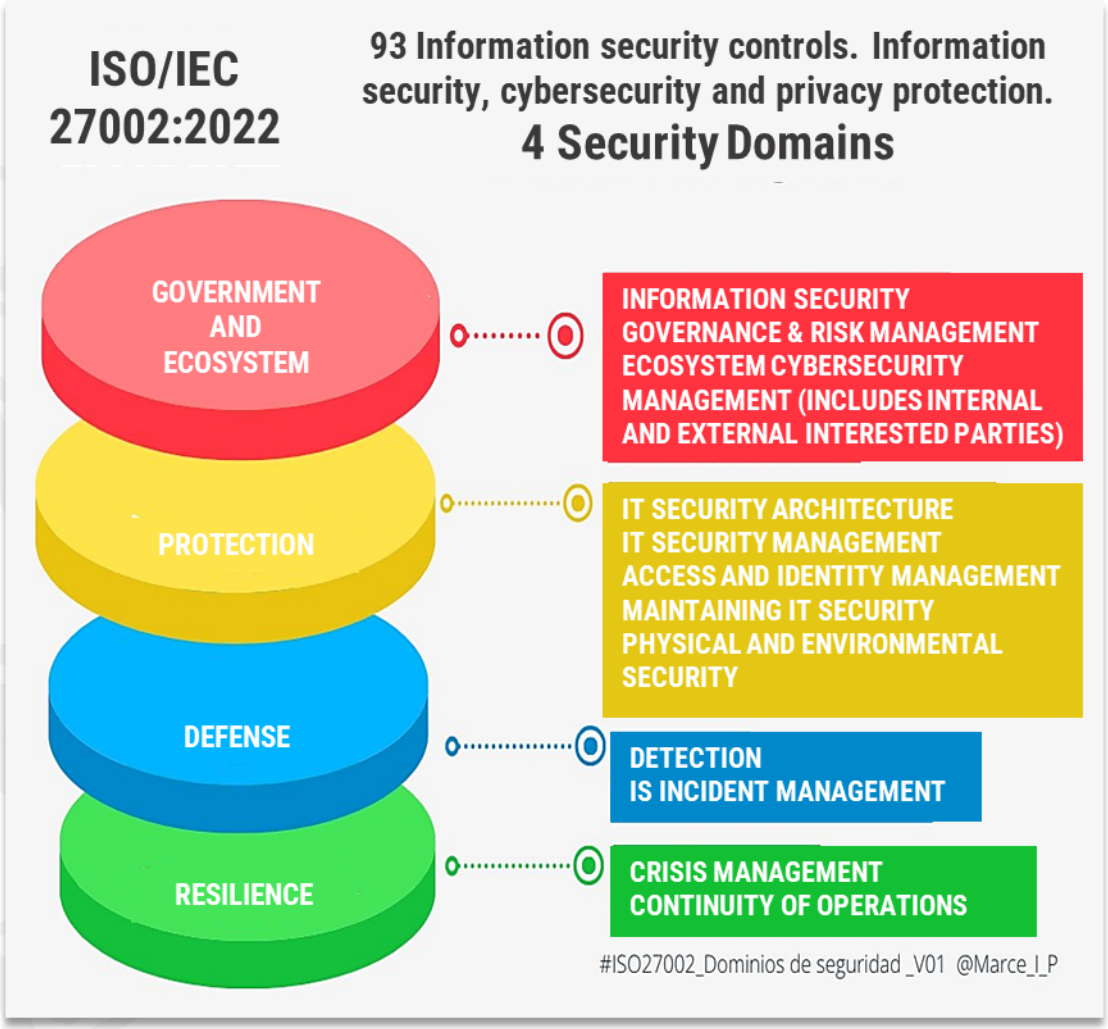
Control: measure that maintains and/or modifies risk

This table shows the 93 ISO 27001 security controls divided in 4 chapters.
Source: https://twitter.com/hackinarticles/status/1714682070960615761

What is the ISO 27002:2022 standard?

Computer Security

- **It is a complement to the ISO 27001 one**
  - It is not a management standard, but **a set of directives and Good practices**
  - Explains **how to implement** the security controls in the Annex A of the ISO 27001
- **Not being a management standard implies**
  - Explains all the controls of the Annex A, **no matter if an organization will use them or not**
  - It is **much more detailed and precise**
    - So, it helps to understand if an organization must apply some security controls or not
  - Organizations **DO NOT** certify against ISO 27002, but ISO 27001
  - More precisely, against the application of the ISO 27001 they do
    - Once all the controls are examined and the ones that are **adequate to be applied are chosen**



Obviously, ISO 27002:2022 uses the same 4-chapter division of controls tan the ISO 27001:2022 it complements. Source: https://twitter.com/Marce_I_P/status/1681992650751111169

How is an ISO 27002:2022 security control like?

- **THEY ARE NOT technical controls**
  - They do not include those type of details, unlike the CIS Benchmarks or STIGs controls
- **Each control has a general description**
  - They are **flexible** regarding its implementation
  - **Depending on the needs** of the organization (size, managed information, legal requisites...)
  - Each control is justified with a **table of 5 associated attributes**
    - We will review them in the following slide
- **Version 2022 is not free and cannot be freely consulted**
  - But we can see how the controls are like using the ones of the previous version
  - Here: https://normaiso27001.es/a9-control-de-acceso/#

Objective 1:
Business Requirements for Access Control
Limit access to information and information processing facilities.

Controls:
- ✓ **9.1.1 Access Control Policy**
- ✓ **9.1.2 Access to networks and network services**

Objective 2:
User Access Management
Secure access by authorized users and prevent unauthorized access to information systems and services.

Controls:
- ✓ **9.2.1 User Registration and Cancellation of Registration**
- ✓ **9.2.2 User Access Management**
- ✓ **9.2.3 Managing Privileged Access Rights**
- ✓ **9.2.4 Managing Users' Secret Authentication Information**
- ✓ **9.2.5 Reviewing User Access Rights**
- ✓ **9.2.6 Removal or adjustment of access rights**

Objective 3:
User Responsibilities
Make users responsible for safeguarding their authentication information.

- ✓ **9.3.1 Use of Secret Authentication Information**

Objective 4:
User Responsibilities
Prevent unauthorized access to systems and applications.

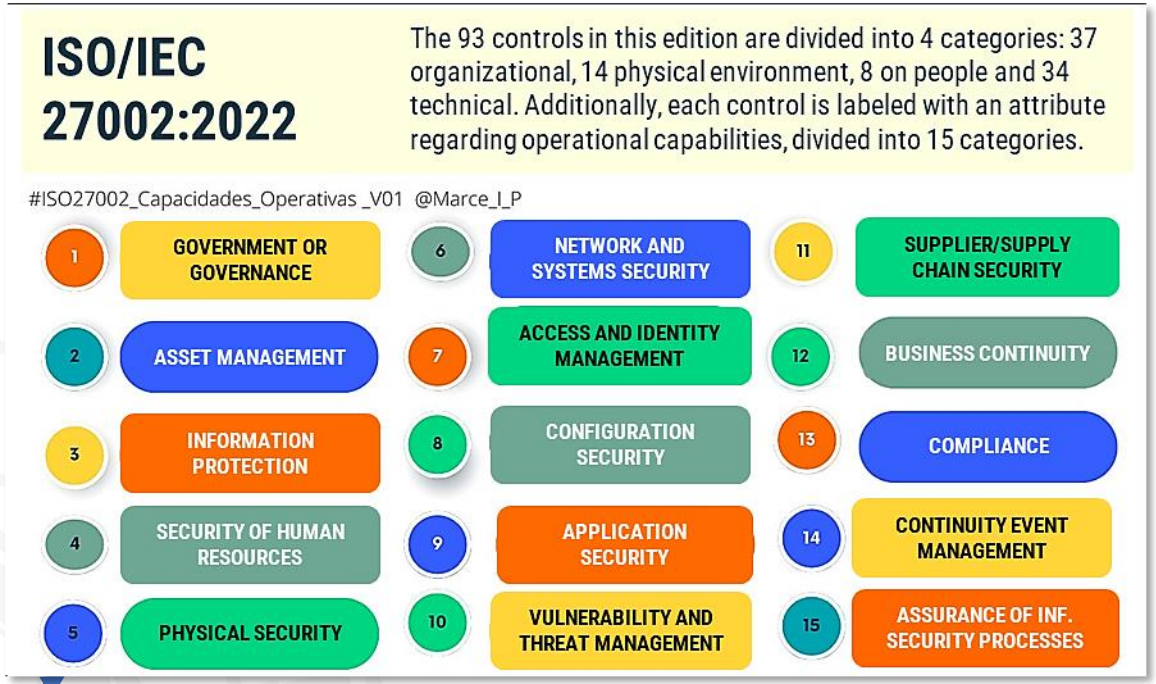
- ✓ **9.4.1 Restriction of Access to Information**
- ✓ **9.4.2 Secure log-on procedures**
- ✓ **9.4.3 Password Management System**
- ✓ **9.4.4 Use of Privileged Utility Programs**
- ✓ **9.4.5 Controlling Access to Source Program Code**

An ISO27002:2013 control gives us an idea of how controls of the 2022 version are: General objectives and open explanation, adaptable to organization requirements

Attributes of an ISO 27002:2022 control

Computer Security

- **Each control has 5 attributes**
  - **Control type** (Preventive, Detective, Corrective)
  - **Information security Properties** (CIA, **Topic 2**)
  - **Cybersecurity concepts** (next slide)
  - **Operational Capabilities** (15, see image)
  - **Security domains** (4)



Operational capabilities of an ISO 27002:2022 control.
Source: https://twitter.com/Marce_I_P/status/1663694032164225027

5.1 Policies for information security

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosystem #Resilience

Control

Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.

Purpose

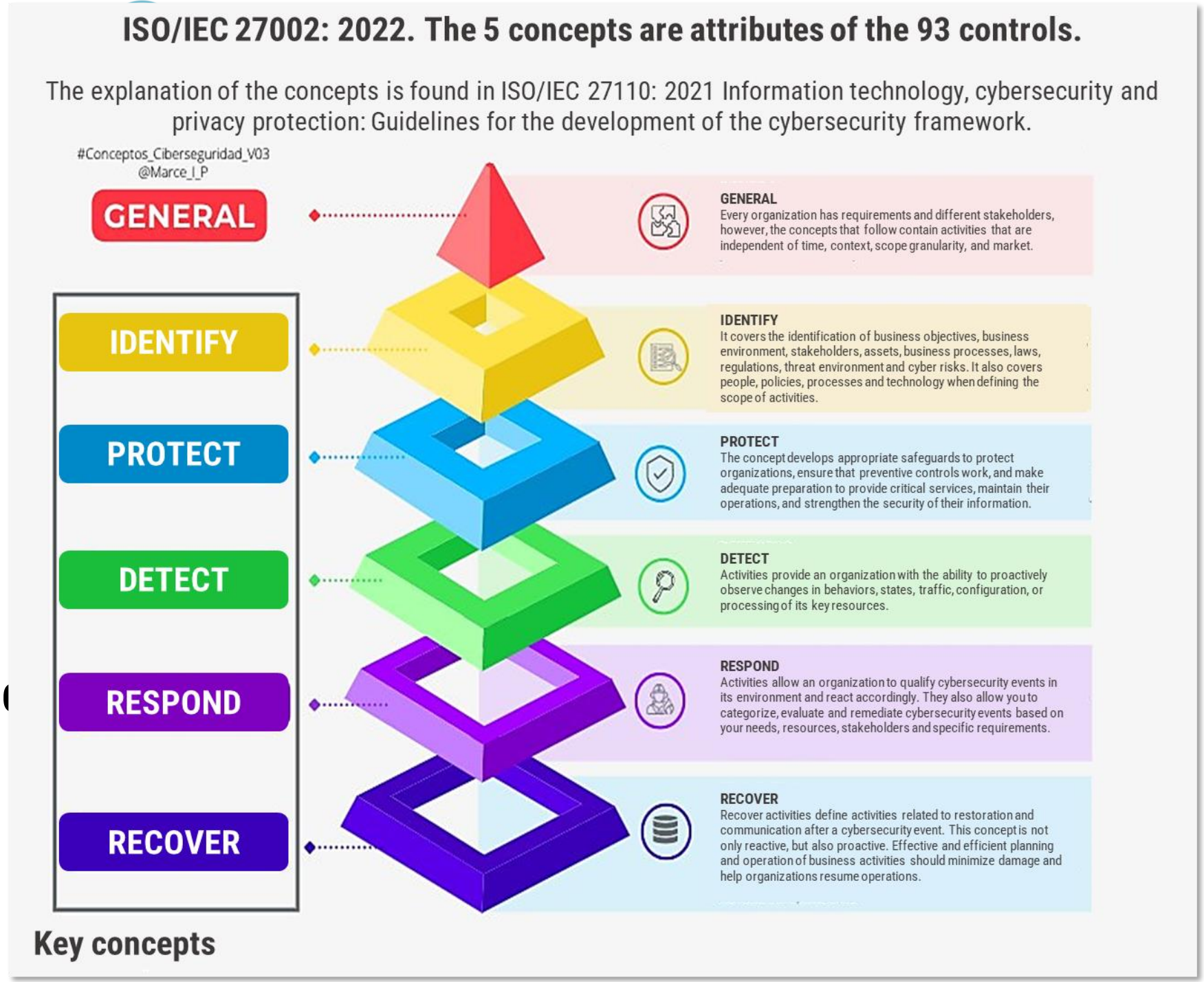
To ensure continuing suitability, adequacy, effectiveness of management direction and support for information security in accordance with business, legal, statutory, regulatory and contractual requirements.

- **Security Domains**
  - Governance and Ecosystem
  - Protection
  - Defense
  - Resilience

Header of the ISO 27002:2002 control 5.1. Source: https://es.slideshare.net/AndreyProzorov/iso-270012022-what-has-changedpdf

Attributes of an ISO 27002:2022 control

- Not all controls serve the same purpose
- Some are more "passive" (identify, detect, protect)
  - Prevent security incidents from happening
- And others that are more "reactive" (respon and recover)
  - They act when security incidents have already occurred



Think you've understood it all? Evaluate yourself!

?

- **You can do the following**
  - *Understand the organization's goals of successfully implementing an ISMS*
    - *And its advantages, both internally and in terms of reputation*
  - *Understand that implementing an ISMS implies that the organization has studied and evaluated its risks, implemented controls (technological or organizational) for those considered most critical, and documented its procedures*
    - *And it has also committed to a process of continuous review and improvement*
  - *Be aware that there are several standards for implementing an ISMS and that ISO 27000 is one* ***About ISO 27000…***
    - *Understand that ISO 27001 is a management standard and that as such you can certify against it*
      - *But it doesn't contain detailed information about security controls*
      - *And that it is the ISO 27002 standard, complementary to the first, that has this information*
    - *Be aware that the controls are organized into four groups and that, unlike those seen in the CIS, they are of a more abstract nature (they affect the organization, people, etc.) and not of a technical nature*
      - *And that, for that reason, it is possible to map them to the CSC controls we saw previously*
    - *Understand that each control has attributes that classify and organize them, so that they can be implemented according to virtually any criteria that the organization needs*
    - *Understand that, on a more abstract level, in addition to general controls, you can find controls focused on different actions that must take place during an attack*
      - *Identify targets, protect yourself, detect activities, respond to problems, and recover from damage*

How ISMS are implemented

Example with the ISO 2700X:2022 international standard

*Icons by Bing Chat AI

Source: Bing Chat AI

What are you going to find in this block?

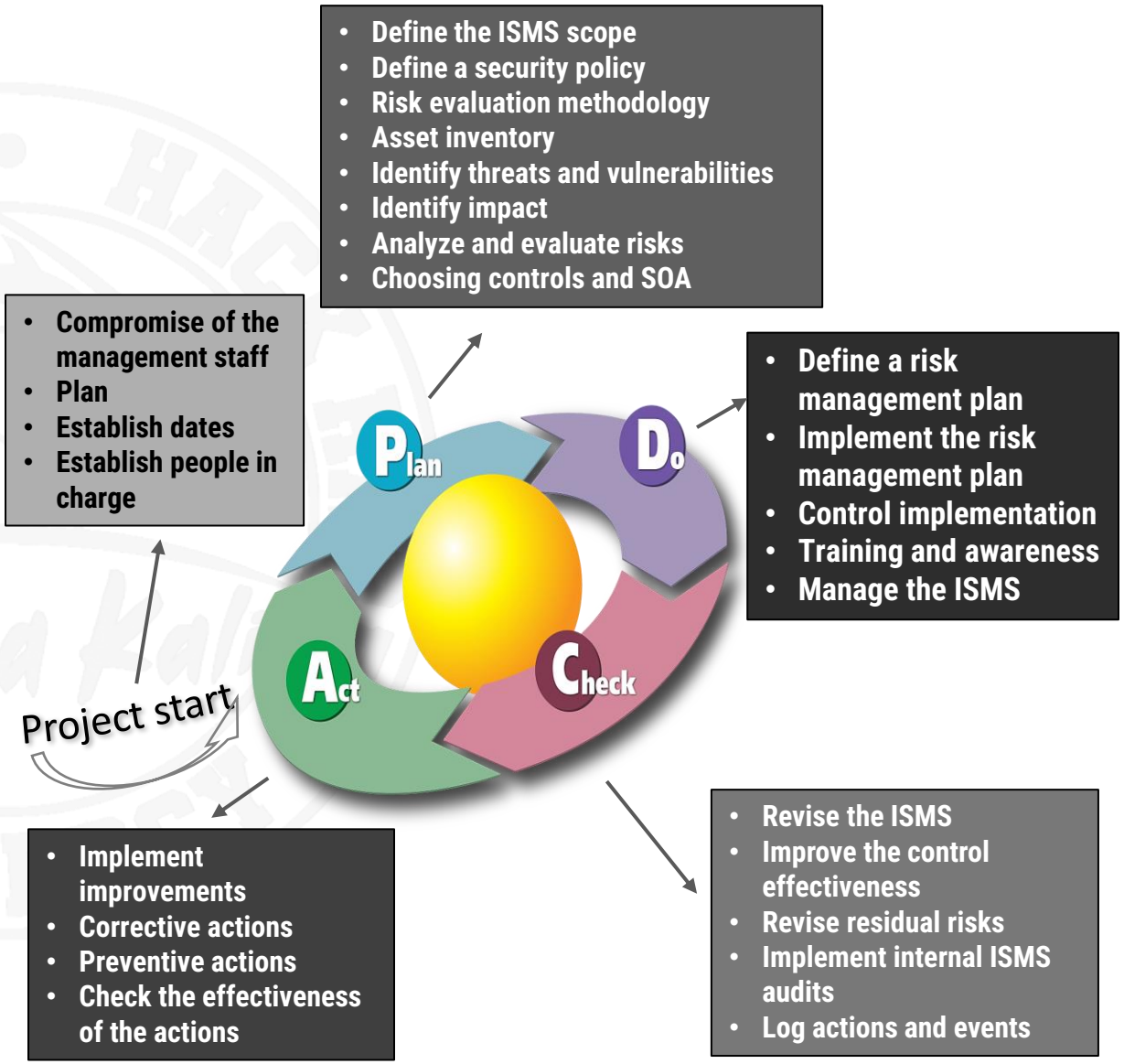
- **In this block you will learn**
  - What the **Deming cycle** is when implementing an ISMS, and its 4 different phases
  - What exactly is done in each **phase** of that cycle
  - The enormous importance of having a good **inventory of an organization's assets**
  - How to **manage a company's risks** at a general level
  - That the implementation of an ISMS is a cycle of **continuous improvement**

ISMS IMPLEMENTATION STAGES (DEMING CYCLE)

- The ISO 27001 standard provides a framework to implement an ISMS in four implementation stages
  1. **PLAN**: Set up the ISMS
  2. **DO**: Implement and use it
  3. **CHECK**: Monitor, review and verify it
  4. **ACT**: Maintenance and improvement of the ISMS

Source: http://www.iso27000.es/sgsi_implantar.html

Based in the "Kaizen" continuous improvement philosophy: https://es.wikipedia.org/wiki/Kaizen



PLAN: DEFINE THE ISMS BOUNDARIES

- ISMS design depends on the **goals, requirements** and **structure** of the organization
- This defines the areas involved in the ISMS deployment
  - Just one department, certain buildings, some business areas…
- Implementation time is not easy to predict (usually 6 months - 1 year) due to
  - Organization size
  - Initial security state
  - Resource investment into the ISMS implementation

PLAN: DEFINE THE ISMS BOUNDARIES. EXAMPLE

- An industrial 3D printing company
- 800 employees (operators, administrative…)
- Multiple departments
  - **Payroll management**: 4 employees
  - **Human Resources** (HR): 3 employees
  - **Systems**: 5 employees
  - **Design**: 8 employees
  - **Production**: rest of employees
- An ISMS is only really needed in departments where sensitive information is handled
  - Payroll management, HR, systems and design
  - 20 employees + CEO only!

Source: https://www.pexels.com/es-es/foto/edificio-blanco-15120-269077/

PLAN: DEFINE THE SECURITY POLICY

- **General guidelines and goals** related to security of the company
  - Formally written and approved by the company management
- Policies must clearly express their goals
  - Frequently involve the participation of a lot of people during their creation and maintenance
- Includes
  - General security **goals and limitations**
  - **Express support and approval** from the CEO / management
  - Organization **security values**
  - **Definition of the general and particular responsibilities** about how to manage information security
  - **References to policy supporting documents**

PLAN: DEFINE THE SECURITY POLICY. EXAMPLE

Objective:
Define general purpose guidelines to ensure adequate protection of the DAPRE information.
Provide support and guidance to management regarding information security, in accordance with the business requirements and relevant laws and regulations.

Applicability:
These are policies that apply to Senior Management, Ministers, Advisors, Presidential Advisors, Directors, Secretaries, Heads of Office, Area Chiefs, officials, contractors, and in general to all users of information that comply with the general purposes of the DAPRE.

Guidelines:

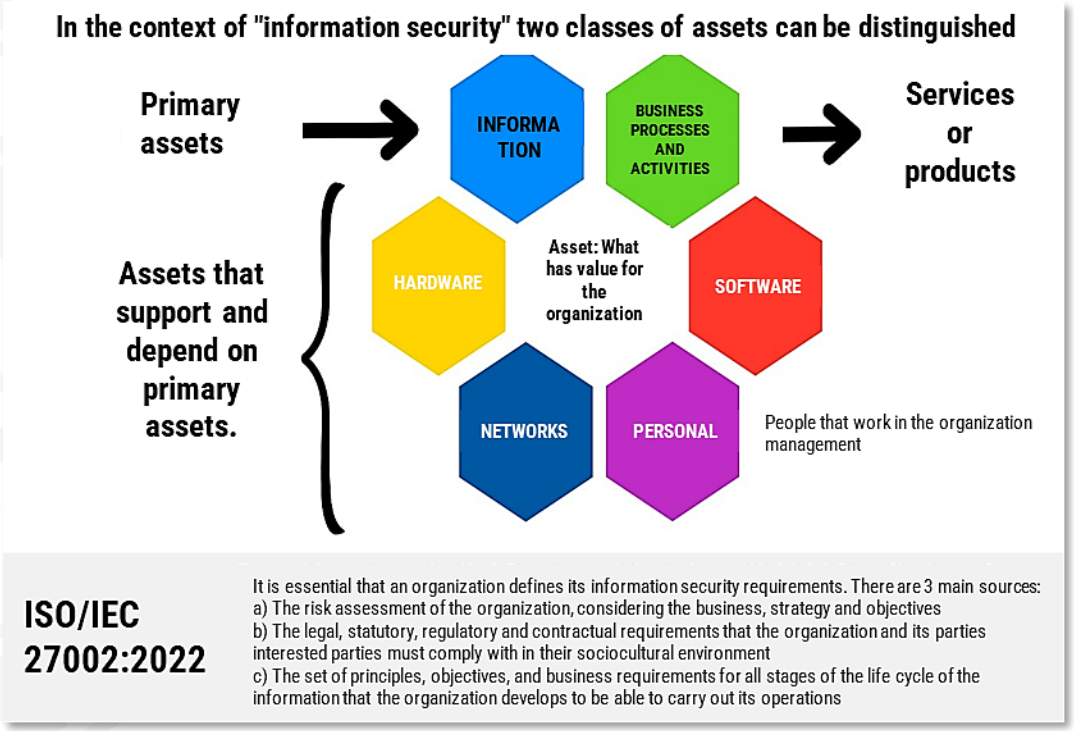
- It must be verified that information security policies are defined, implemented, reviewed and updated.
- Design, program and carry out the audit programs of the Information Security Management System, which will be in charge of internal control.
- All computer applications or software must be purchased or approved by the Information and Systems Area in accordance with the entity's procurement policy in accordance with **process C-BS-07 Acquisition of Goods and Services**.
- The DAPRE must have a firewall or perimeter security device to establish connections to the Internet or when it is unavoidable for connection to other networks in outsourcing or third parties.
- The remote connection to the DAPRE local area network must be made through a secure VPN connection provided by the entity, which must be approved, registered and audited, except in cases authorized by the Information and Systems Area.
- The area or unit head employees must ensure that all information security procedures within their area of responsibility are carried out correctly to achieve compliance with the information security policies and standards of the DAPRE

Source: http://wp.presidencia.gov.co/sitios/dapre/sigepre/manuales/M-TI-01%20Manual%20general%20Sistema%20de%20Seguridad%20de%20la%20Informacion.pdf

PLAN: DEFINE ASSETS

- Assets are **key resources** to ensure proper operation of the organization
- Therefore, they are anything valuable enough to be protected
  - Information
  - Buildings
  - Computer systems and networks
  - Applications
  - Databases
  - Storage media
  - … (see image)

ISO 27002:2022 assets.
Source:
https://twitter.com/Marce_I_P/



- Asset definition must include
  - An **inventory**: Description, localization, owner…
  - **Dependencies** between assets
  - Asset **rating**, depending on how relevant they are and the potential impact they may have if any incident occur over them

PLAN: DEFINE ASSETS. EXAMPLE

- **Typical asset inventory**

Source: https://www.metrici.com/metrici/forum/threads/Thread4

ISMS.online Search Home You Work David

Tracks ▸ Information Asset Inventory (ISO 27001)

Information Asset Inventory (ISO 27001)

Linked work Team Settings Tour

Showing: 16 of 16 Summary value £0.00 (from total £0.00)

View Archive View Updates feed View Stats New Item

Assigned to: All Team Members Category: Status All Statuses View: Columns List

Name	Status	Primary Location	Legal Owner	Classification	Owner/Lead	Type	Assigned To	Due
2 - Laptops: company provided	Live	Company Office On Person Teleworker (Home)	Company	Commercial in Confidence	CTO	Processing Devices	David Kelly	07/01/19 11:00
7 - Brand	Live	Everywhere	Company	Commercial in Confidence	CMO (marketing)	Sales & Marketing IPR	David Kelly	07/01/19 12:00
8 - Company financial data	Live	Company Office	Company	Commercial in Confidence	FD	Financial information	Karen Arnold	07/01/19 14:00
13 - Product X code base	Live	Third Party Datacentre	Company	Infrastructure Critical	CEO	Products & Services Infrastructure IPR	Gill Smith	07/01/19 14:00
9 - Product marketing materials (published)	Live	Everywhere	Company	Public	CMO (marketing)	Products & Services Sales & Marketing IPR		07/01/19 18:00
1 - Staff personal data	Resolved	Company Office	Company	Commercial in Confidence	HR	Personal Data		
3 - Laptops: Infrastructure Critical focused	To-do							
4 - Laptops: BYOD (employee)	To-do							
5 - Mobile Phones: company provided	To-do							
6 - Mobile Phones: BYOD (employee)	To-do							

Third Party Datacentre
Other Location

Legal Owner
Company
Employee (inc.BYOD)
Supplier
Customer
Other

Classification
Infrastructure Critical
Commercial in Confidence
Public
Unknown

Owner/Lead
CEO
DPO

Uncategorised

Clear all options Apply filter

PLAN: RISK ANALYSIS

- **Probability that a threat may exploit a vulnerability** and cause damages or total loss of an asset
- They are usually expressed combining the probability of an event and their consequences
- There are several risk evaluation and analysis methodologies nowadays
  - The ISO 27001 standard do not force to use a concrete one
  - MAGERIT is commonly used in the Spanish administration
- This is just a brief outline of something that will be analyzed in more detail in a future course (DPPI, 4th year)

PLAN: RISK ANALYSIS

- To calculate **identified assets risk levels**, we need to
  - Identify **threats** to assets covered by the ISMS
  - Identify **vulnerabilities** that could be exploited by threats
  - Identify and evaluate the **impact** (cost) of a failing asset
  - Evaluate the **probability of failure**
    - Considering the 3 previous elements
  - Calculate **risk levels** using an objective method
  - Determine if calculated risk are **acceptable** or some action is required

THREAT	VULNERABILITY
Attack by a cybercriminal organization / individual	A configuration problem allows connection to private services evading firewall rules
	XSS due to lack of proper validation leading to script execution
	XST caused by a filtering error and using the TRACE HTTP verb
Computer overheat	No temperature monitoring controls
Server information leak	Default Tomcat installation
Fire	No fire extinguisher in the building

Asset	Threat	Vulnerability	Impact			Probability	Risk	Risk Classification
			Confidentiality	Integrity	Availability			
Laptop	Theft	Portability	2	3	1	1	3	
File server	Malware	Lack of updates	3	3	3	1	4	
Client contract	Theft	No safe to store documents	4	4	1	2	5	
Client data	Leak	No authenticated access	5	4	3	2	6	

PLAN: RISK MANAGEMENT

- **Identify and evaluate alternatives to treat risks** with any of the following goals
  - **Eliminate** the risk
    - E. g.: remove an obsolete server
  - **Mitigate** the risk
    - E. g.: apply technical security controls to eliminate it
  - **Transfer the risk management** to an external agent
    - E. g.: subcontract the server maintenance service
  - **Assume** the risk (you can't currently deal with it)

- Finally, the **residual risk** must be analyzed
  - Existing risk level after safeguards have been implemented
- ISO 27001 control implementation depends on the results of the organization risk analysis
  - The standard only requires that the organization implement **those that are really needed**
  - According to the identified risks, their **impact**, and their **probability** of failure

PLAN: DEFINE CONTROLS AND PROCEDURES

Computer Security

- **Control**
  - Measures, actions, and documents allowing auditing and covering a risk
- **Procedure**
  - Implementation instructions of tasks / processes of a control
  - Establishes the steps to follow to implement the tasks concisely
- **Statement of Applicability (SOA) document, containing**
  - The control **goals**
  - **What have been chosen** from the standard
  - **Why** these controls have been chosen
  - The adopted **security measures**

Before the certification audit, an organization must have produced a Statement of Applicability (SOA).

The requirement is outlined in the ISO 27001. The SOA must contain at least 93 entries with each of the categories and controls listed. Once this is done then each control must be either selected and justified or excluded with similar justification. All SoA documents must be able to demonstrate that consideration has been given to each control. This means that an SoA must contain all entries outlined, simply listing selected controls will not meet the requirement.

This example here shows how a difference between a selected and excluded control could be presented within a SoA:

Statement of Applicability — Current as of

Legend (for Selected Controls and Reasons for controls selection) — Version X-Date of Document

ISO 27001 Controls				Current Controls	Remarks (including justification for exclusion)	Remarks (Overview of implementation)
Clause	**Sec**	**Control**	**Objective/Control**			
	9.4.2	Secure log on procedures	Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure	**Policy**	Secure log on required for all systems and application access.	Document Organisations ISMS Manual and Index version 1 dated 2 Aug 20 provides guidance
	9.4.3	Password management system	Password management systems shall be interactive and shall ensure quality passwords	**Policy**	All systems, platforms and applications require passwords	Document Organisations Password Policy version 1 dated 2 Aug 20 provides guidance
	9.4.4	Use of privileged utility programs	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled	**Exempt**	Utility Programs not used	
	9.4.5	Access control to program source code	Access to program source code shall be restricted	**Exempt**	No program source code is used.	
	A.10	**Cryptography**				
	10.1	Cryptographic controls	**OBJECTIVE**: To ensure proper and effective use of cryptography to protect the confidentiality authenticity and/or integrity			

Source: https://www.nqa.com/es-es/certification/standards/iso-27001/implementation

PLAN: WHAT IS A SOA EXACTLY?

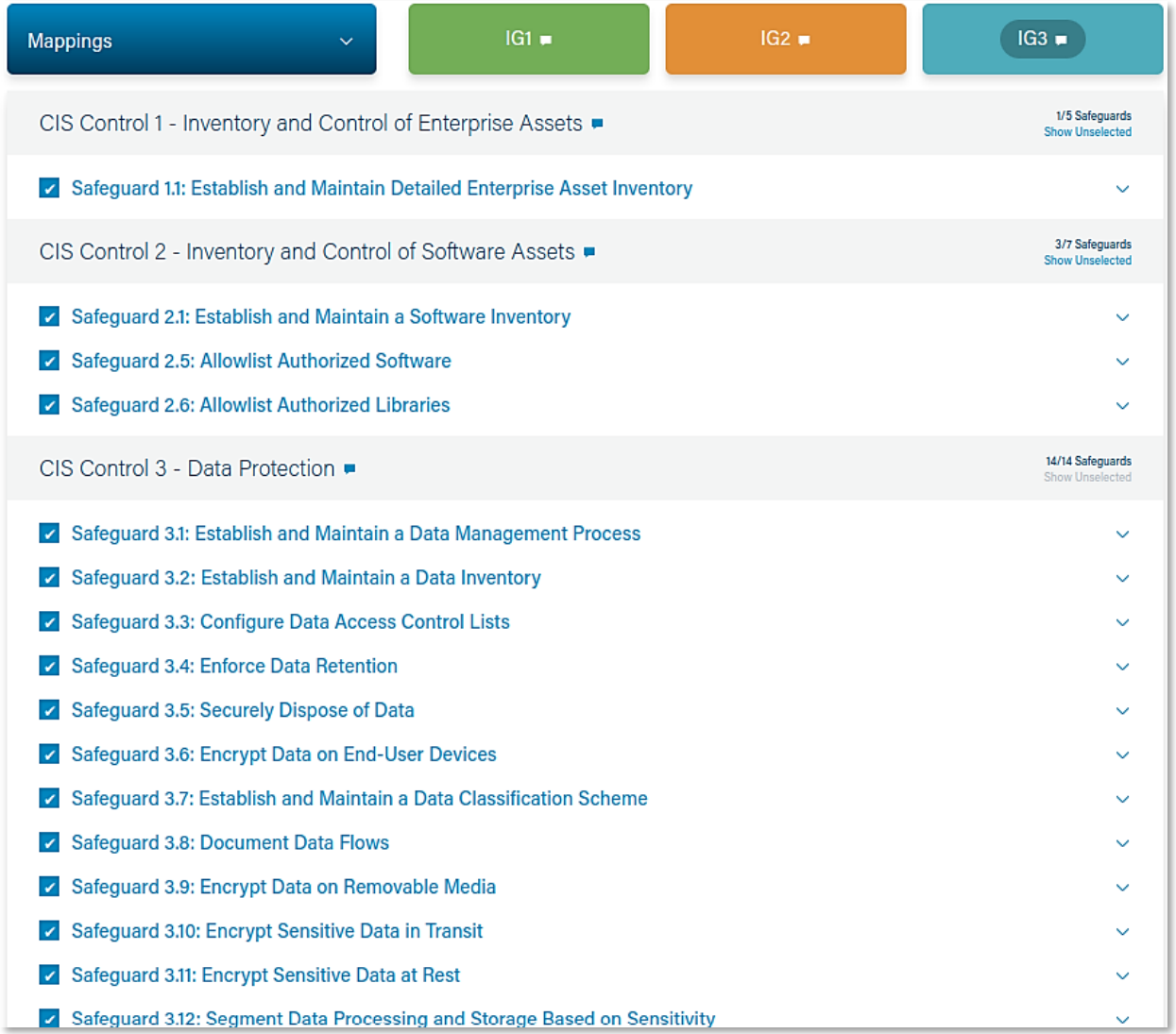
- **After the risks analysis and assessment, we must define the options to manage risks**
  - And apply the security measures to mitigate them
- **The SoA is defined in this step, being a key document of the ISO 27001 standard**
  - Contains a **full list of Annex A security controls**
  - For each controls, it indicates whether it is applicable or not
    - Detailing the reasons and their implementation status
    - It can **add other controls** and control goals if deemed it necessary
    - **Remember**: the standard is flexible and adapts to the needs and particularities of the organization
  - The SoA enables **traceability between controls**
    - And a broad view of what the organization is doing to protect your information
    - Contributing to the identification, organization and registration of the implemented security measures

PLAN: DEFINE CONTROLS AND IMPLEMENTATION PROCEDURES

- **Now that the ISO controls that are going to be applied are chosen thanks to the SOA, we require a detail on how they are going to be implemented (technical procedures)**
  - **Consulting with information security experts**: They will provide the detailed technical guidance on how to implement organization-specific security controls
  - **Training & Certification**: Courses that provide the technical knowledge needed to implement them
  - **Online Resources and Literature**: That may provide you detailed technical guidance
    - STIG, ENS (remember that they have detailed procedures) and, especially, **CSC controls**
    - Remember that **CSC controls can be mapped to ISO 27001 ones**, among other frameworks
      - They allow you to comply with multiple frameworks by implementing a single technical procedure
    - Keep in mind that mapping is not always perfect, and **should be carefully reviewed** to ensure that the ISMS requirements identified above are being met
    - Always in accordance with the ISO 27002:2022 document for each control
  - **Security tools and software**: Many security tools and software can help you implement specific security controls

PLAN: DEFINE CONTROLS AND IMPLEMENTATION PROCEDURES

- As we said, CIS Controls can be mapped to ISO 27001 controls
- And our work with CIS Benchmarks can facilitate compliance with the ISO 27001 standard
  - We implement part of its controls through the CIS Benchmarks contents
- Not every ISO 27001 control has a corresponding CSC control
  - If the organization need to implement one of these, we have to use one of the three information sources previously outlined



Source: https://www.cisecurity.org/controls/cis-controls-navigator/

PLAN: DEFINE CONTROLS AND IMPLEMENTATION PROCEDURES

Ubuntu 22.04 CIS Benchmark (PDF) → **CSC Controls v8 (and their Safeguards)** → **Map to*** → **ISO 27001:2022 security controls**

Every technical security control of the Safeguard 3.3

CSC Control 3 – *Data Protection*

- ***Safeguard 3.3***: *Configure Data Access Control Lists*

→ **5.10 Acceptable use of information and other associated assets**
5.15 Access control
8.3 Information access restriction
8.4 Access to source code

Every technical security control of the Safeguards 4.3 and 4.8

CSC Control 4 – *Secure Configuration of Enterprise Assets and Software*

- ***Safeguard 4.3***: *Configure Automatic Session Locking on Enterprise Assets*
- ***Safeguard 4.8***: *Uninstall or Disable Unnecessary Services on Enterprise Assets and Software*

→ **8.5 Secure authentication**
8.9 Configuration management

Every technical security control of the Safeguards 8.2 and 8.9

CSC Control 8 – *Audit Log Management*

- ***Safeguard 8.2***: *Collect Audit Logs*
- ***Safeguard 8.9***: *Centralize Audit Logs*

→ **8.15 Logging**
8.20 Networks security

→ **There are no mapping (but can be added to the SoA if the organization deemed it necessary**

Source: https://www.cisecurity.org/controls/cis-controls-navigator, mapped to ISO 27001 & 27002, IG3

PLAN: CREATE THE FINAL SECURITY PLAN

- **Every created activity generates a final document**
  - It reflects the actions that will be taken to implement the security controls chosen to create the ISMS
- **This plan covers short, medium and long-term actions, also including**
  - Security **goals**
  - **Responsibilities** (who is in charge of what)
  - **Budget**
  - **Estimated resources** (HR, materials…) and **timetable** to implement the actions

DO: IMPLEMENT RISK MANAGEMENT PROCEDURES

- **We have chosen which ISO controls are going to be implemented (SoA)**
  - And, if we used the CSC Controls, we also defined that multiple ISO controls can be mapped to CSC Controls
- **The next phase consist on implementing the controls and procedures**
  - But, *do you remember that we said that there are ways of automating technical security controls?*
    - This is the goal of the **SCAP protocol** and its implementations (STIGs, `scap-security-guide`, CIS Bencmarks)
  - *Do you remember that even each CIS Benchmark technical control indicates if its Audit and Remediation procedures can be automated?* *5.3.3 Ensure sudo log file exists (Automated)*
  - The **technical security controls automation technologies** we reviewed can be of great help for the ISMS technical implementation
    - **We transform command-line commands into things of a greater abstraction level!** ☺
    - After detailing the **PLAN** phase, the time we spend in the **DO** phase **can be greatly reduced** thanks to this kind of **automation technologies**
- **This phase also contemplates resource, responsibility and priority assignments**

DO: USER TRAINING

- **Users must be adequately trained** in the ISMS
  - Training and **security awareness courses** regarding information security must be created
    - Especially against cyber fraud, that is a major threat nowadays
  - Includes **how to properly perform their assigned tasks** and the implemented controls
  - Must be given to **all** employees directly involved in the ISMS
  - But all company employees must be aware of the security implications of their actions and possible threats
- **There is no successful ISMS without proper training and awareness of all employees** in the organization
  - We gave some elements for training in cyberfraud prevention in the topic of **Theory 3**

CHECK: MEASURE CONTROLS EFFECTIVENESS

- **Information security controls implementation must be a continuous effort**
  - That implies to monitor and review its effectiveness regularly
  - And make adjustments if necessary
- **Hence, a system to measure the results obtained from applying controls must be defined**
  - These results must be **reproducible and comparable** to measure how successful they are
  - It is like testing, but for our ISMS instead of our programs ☺
- **Examples**
  - **ISO 8.20 control: Network security** : Firewall stats -> attempts to access forbidden web pages
  - **ISO 8.24 control: Use of cryptography** : Percentage of systems that handle sensitive or valuable data and use proper cryptography methods

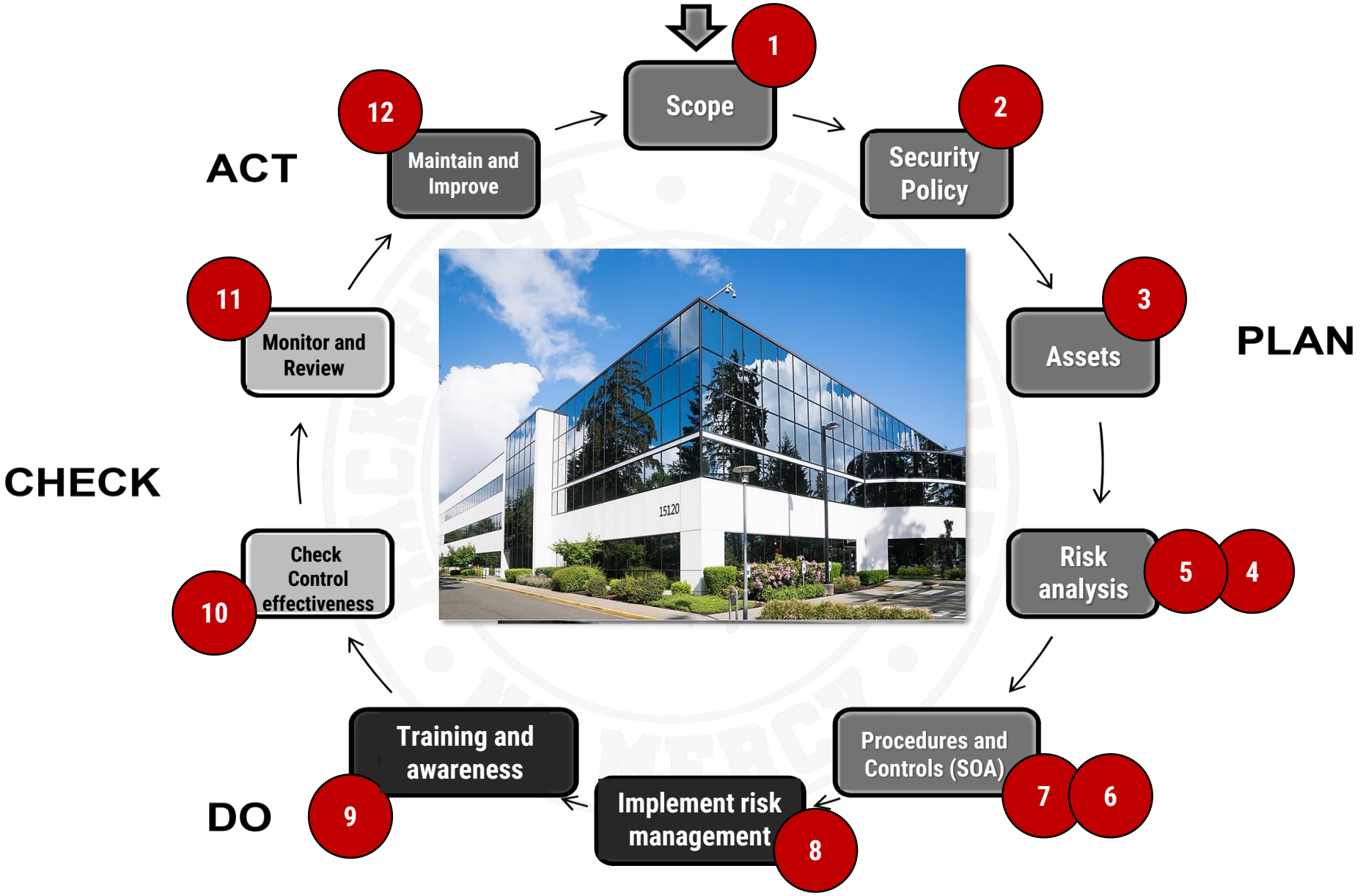
CHECK: MONITOR AND REVIEW

- **Run monitoring and review procedures over the ISMS**
- **Regularly review its effectiveness, considering**
  - The **compliance** with their objectives
  - **Results of security audits**
  - **Incidents**
  - The results of the control **effectiveness measurements**
  - **Suggestions and observations** of all parties involved
- **Regularly review risk assessments, residual risks and acceptable levels at planned intervals, considering possible changes**
  - Considering the possible changes that the organization has undertaken
  - Periodically perform ISMS **internal audits** at planned intervals
  - Review the ISMS periodically by **management employees**
    - To ensure that the **defined scope** remains adequate
    - And that improvements in the ISMS processes are evident

ACT: MAINTAIN AND IMPROVE THE ISMS

- **The organization shall regularly**
  - Implement the identified **improvements** in the ISMS
  - Perform appropriate preventive and corrective actions in relation to the **continuous improvement clause** 8 of ISO 27001
    - Considering everything learned from the experience itself and from other organizations
  - **Communicate actions and improvements** to all stakeholders
    - In the appropriate level of detail
    - And agree, if relevant, about how to proceed
  - Ensure that the improvements that are made **meet the intended goals**

SUMMARY: ISMS IMPLEMENTATION



Source: https://www.pexels.com/es-es/foto/edificio-blanco-15120-269077/

ISO 27001 vs ENS

Computer Security

ISO 27001

- **International and Certifiable Voluntary Standard for any information security management system**. It can be "mandatory" by customer and market requirement.
- Managed by **ISO - International Organization for Standardization.**
- Certifications with **accredited certifiers** are always recommended.
- The certificate is issued for **3 years**. At 12 and 24 months, a follow-up external audit must be done. An annual internal audit is mandatory.
- **There are no** categories or levels within the standard.
- ISO 27001 responds to the **PDCA-Continuous Improvement Cycle model**. We may be in the process of complying with certain controls as long as they are justified. The modulation of the measures is at the discretion of the auditor.
- **ISO does not certify products**. The scope is the "Information Security Management System that supports..."

ENS

- **Mandatory legal provision for information systems** for the public sector and for private companies working for the public sector.
- Managed by the **CCN-CERT - National Cryptologic Centre**, under the Ministry of Defense.
- Certification bodies must be **accredited by the CCN.**
- The certificate is issued for **2 years**. There are no interim audits. They are always "initial audits". An annual internal audit is mandatory.
- There are three **categories: basic, medium, and high.**
- The ENS sets out a series of organizational, documentary and technical requirements to be met. **It is mandatory to meet 100% of the requirements** based on the system category to pass the certification audit.
- We can focus the **scope on specific products or general services provided** by the organization.

Source: https://www.linkedin.com/in/v%C3%ADctor-carmona-esteban-4112a717/?originalSubdomain=es

Think you've understood it all? Evaluate yourself!

?

- **You can do the following**
  - *Understand the four phases of the Deming cycle and what each of them generally does*
  - *Understand that the implementation of an ISMS is an ongoing job, and its initial implementation typically takes several months*
  - *Understand that an ISMS should only apply to employees who handle sensitive information*
  - *Understand the general contents of a security policy*
  - *Be clear that control of all assets is key to being able to implement an ISMS*
    - *And that the term "organization's asset" means many things, not just machines*
  - *Understand the concept of risk, how it is calculated, and what four things can be done when responding to the risks that have been identified*
  - *Understand what you might find inside an SOA document*
  - *Understand that, once the security controls to be implemented are chosen, we must implement them*
    - *And that's where the seen CSC controls connect*
    - *Or other resources that guide us on how to implement them reliably (STIG, ENS...)*
  - *Definitively understand how the security automation seen in this topic can be key when it comes to streamlining the implementation of an ISMS*
    - *Along with the importance of user training, which should be included in it*
  - *Understand that, after implementation, a procedure for measuring the effectiveness, monitoring and review of security controls is necessary*
    - *Before starting the Deming cycle again to continue improving the implemented ISMS*
    - *Understanding that we can only improve things that we measured 1st and known by underperforming*

< Go to Index

Security audit and review methodologies

How can we use them?

*Icons by Bing Chat AI

Source: Bing Chat AI

FROM SECURITY CONTROLS TO METHODOLOGIES

Using a **Security Audit Methodology** (like **OSSTMM**) to review systems security and compliance with the implemented security frameworks

Managed by

Map the implemented controls and **Safeguards** to a worldwide-recognized **Security Framework** (ISO 27001, PCI-DSS…) to facilitate the implementation of an **ISMS**

Map to

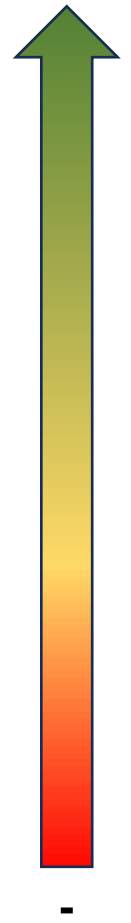
Use **Implementation Groups** (only 3) to implement only the most adequate **Safeguards** for my scenario, according to my resources

Can be distributed into

Group the implemented security controls in **CIS Critical Security Controls (CSC)** and **Safeguards**

Can be grouped into

Check and implement adequate and validated **technical security controls** in a software product / OS in a highly **automated** way (several hundreds)



DIAGNOSING SECURITY

- **It is necessary to perform an exhaustive security test on each section that have security concerns to initiate any of the ISO 27001 phases**
  - This will determine the **vulnerabilities of the organization's assets**
- **The OSSTMM (Open-Source Security Testing Methodology Manual) security audit methodology can be used for that**
  - It is one of the most comprehensive and commonly used professional standards to review systems security
  - Provides a standardized method to perform exhaustive security tests to each security-related section of an organization
  - Also covers compliance with standards and best practices such as those set out by ISO 27001 – 27002, NIST, or ITIL

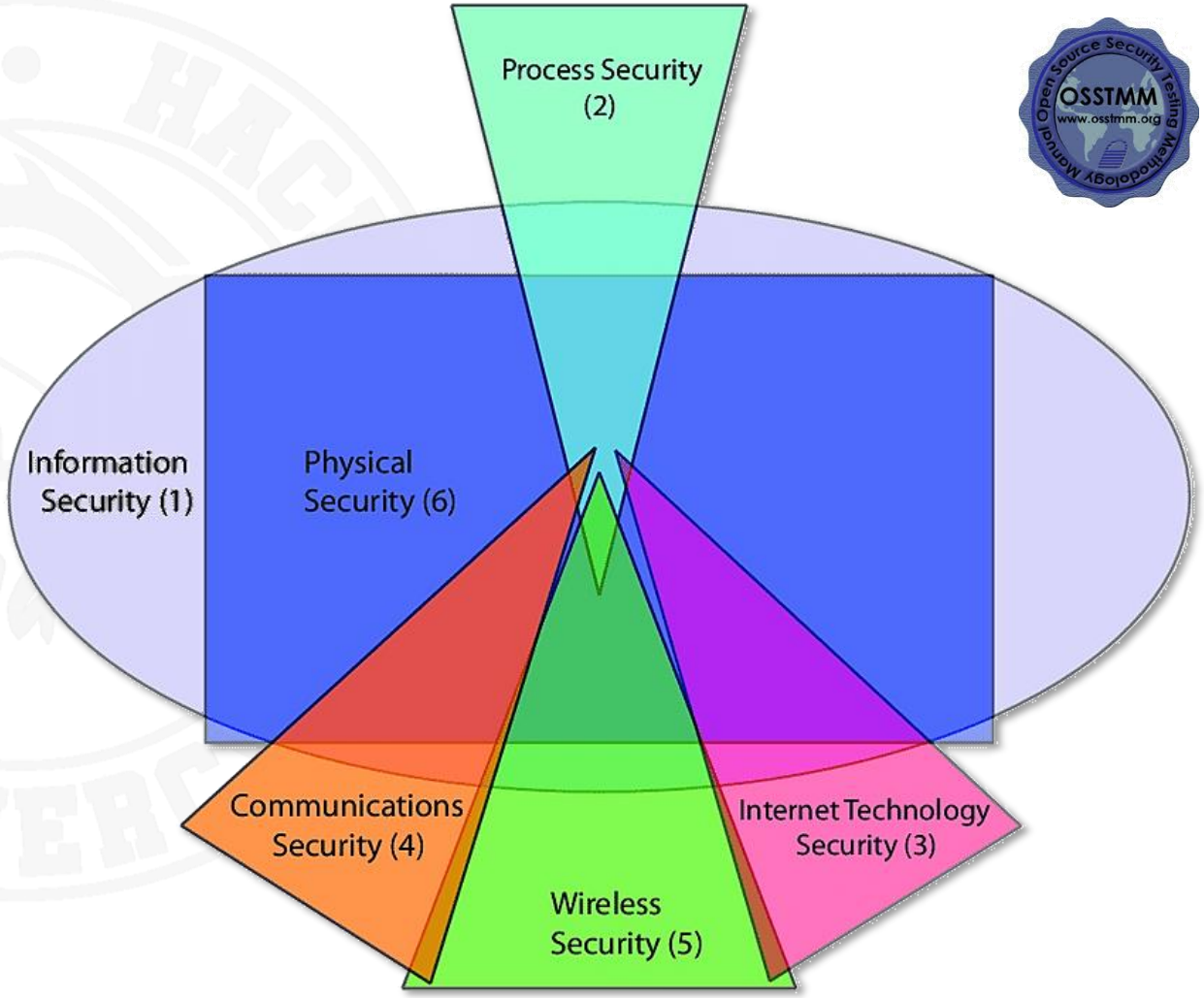
What is OSSTMM?

- Methodology developed by ISECOM to carry out tests, analysis and measurement of real operational security
  - In other words, it is a **methodology for conducting technical security audits**
- It's designed to be consistent and repeatable
- Allows any security audit professional to contribute proposals for security testing
  - So that they can be more precise, concrete and efficient
- It also allows the free dissemination of documentation without intellectual property problems

OSSTMM SECTIONS

Source: https://www.researchgate.net/figure/The-figure-illustrates-the-security-testing-sections-in-the-Open-Source-Security_fig6_268418932

- **The sections with security-related concerns are**
  1. Information Security
  2. Process Security
  3. Internet Technology Security
  4. Communications Security
  5. Wireless Security
  6. Physical Security
- **Version 3 (final) can be downloaded here**
  - https://www.isecom.org/OSSTMM.3.pdf



OSSTMM MODULES

- Each section is composed by modules. Example

Security in Internet Technologies

- …
- Intrusion Detection System (IDS) review
- Network probe
- Services and systems reconnaissance
- Testing internet applications
- Password decryption
- Denial of Service test
- …

- Each module is described, proposes a series of actions, and enumerate their expected results

OSSTMM: Password decryption example

Description

- Decrypting passwords is the process of validating password robustness using automated password recovery tools
- These could expose
  - Usage of **weak cryptographic algorithms**
  - **Incorrect implementations** of these algorithms
  - **Weak passwords** due to human factors
  - …

Expected results

- Decrypted and undecrypted **password files**
- **List of accounts** (users or system, **Topic 3**) with passwords
- **List of vulnerable systems** to password decryption attacks
- **List of vulnerable files or documents** to password decryption attacks
- List of systems with user or system accounts **using the same passwords**

OSSTMM: Password decryption example

- **Verification actions**
  - Obtain the system password file
  - Initiate an **automated dictionary attack** on the password file
  - Initiate a **brute force attack** on the password file
  - Use the obtained passwords or variations of them to **access additional systems** or applications
  - Use **automated decryption programs** against encrypted files that have been found (PDF, Office documents, compressed files…) to attempt to collect more data
  - **Check the date** when the passwords were set
- **These actions are performed with tools we will describe in the pentesting block of this course** (Topic 7)

INCIDENT RESPONSE (IR)

Computer Security

- It is an organized plan to know **what to do against certain security incidents**
  - Preparation, detection and analysis, containment, eradication, recovery, learning and testing
- Learning and maturity process while an organization gains experience in cybersecurity management
  - "Our organization operations manual in case of cyber-catastrophes" ☺
- There are company IR evaluation methodologies like the CREST one
  - https://www.crest-approved.org/cyber-security-incident-response-maturity-assessment/index.html

INCIDENT RESPONSE FOR COMMON ATTACK TYPES

Attack Name	What It Is?	Threat Indicators	Where to Investigate	Possible Actions
Brute Forcing	Attacker trying to guess a password by attempting several different password	Multiple login failures in a short period of time	Active Directory Logs Application Logs Operational System logs Contact User	**If not legit action**, disable the account and investigate/block attacker
Botnets	Attackers are using the victim server to perform DDOS attacks or other malicious activities	Connection to suspicious IPs. Abnormal high volume of network traffic	Network Traffic OS Logs (New processes) Contact Server Owner Contact Support Team	**If confirmed:** Isolate the server Remove malicious processes Patch the vulnerability utilized for infection
Ransomware	A type of malware that encrypts files and reuests a ransom(money payment) from the user to decrypt the files	User contacting; Burst of "file update"logs Anti Virus alerts Connection to suspicious IPs.	AV Logs OS Logs Account Logs Network Traffic	Request AV Checks Isolate the machine
Data Exfiltration	Attacker (or rogue employee) exfiltrate data to external sources	Abnormal high network traffic Connection to cloud-storage solutions(Dropbox, Google Cloud) Unusual USB Sticks	Network Traffic Proxy Logs OS Logs	**If rougue employee:** Contact manager, perform full forensics **If external Threat:** Isolate the machine, disconnect from network
Compromised Account	Attackers get access to one account (via social engineering or any other method)	Off-hours account logins, Account group changes, Abnormal high network rtaffic	Active Directory Logs, OS Logs, Network Traffic, Contact User for Clarifications	**If confirmed:** Disable Account, Password Changes, Forensic investigations
Denial Of Service (DoS/DDos)	When attacker is able to cause interference in a system by exploiting DoS Vulnerabilities or by generating a high volume of traffic	Abnormal high network traffic in public facing servers	Network traffic, Firewall Logs, OS Logs	**If DoS due to vulnerabilities:** Contact patching team for remediation. **If DDoS due to network traffic:** Contact network Support or ISP.
Advanced Persistent Threats (APTs)	Attackers get access to the system and create backdoors for further exploitation. Usually hard to detect.	Connection to suspicious IPs, Abnormal high volume of network tarffic, Off-hours access logs, New Admin account creations.	Netwotk traffic, Access Logs, OS Logs (new processes, new connections, abnormal users), Contact server owner/support teams.	**If confirmed;** Isolate the machine, start formal forensics process, Start escalation/commuication plan.

And now?

- **Implementing a full ISMS is beyond the scope of the course**
  - Risk management is part of a future course (DPPI, 4th year)
  - Law-related topics is also part of another future course (ASLEPI, 4th year)
- **But we saw ways to automate its practical outcome: computer systems hardening**
  - Automate the evaluation and remediation of the potential security vulnerabilities we detected
  - Have **trustable information sources to secure OS and common software products** (Firefox, Chrome…) following a series of guidelines
  - Know how to use this work to facilitate “getting serious” and implement security frameworks on a documented and professional way
  - This way, we have a way to quickly achieve hardening of a system in an efficient way
  - And, with time, scale this to implement something more complex on a higher abstraction level
  - Best of both worlds! ☺

TOPIC 4
SECURITY POLICIES AND AUTOMATED HARDENING