TOPIC 4. SECURITY POLICIES AND AUTOMATED HARDENING

Defense against the dark arts

José Manuel Redondo López *"S-81 Isaac Peral"* Project v3.0

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo

Logo: @creative_vanesa (*Instagram*)

INDEX

< Go to Index

ENS >

SCAP >

SECURITY HARDENING AUTOMATION

Hardening could not be hard

What is this topic?

José Manuel
Redondo López

- **At the end of the previous topic, we outlined two key elements to achieve proper security with less effort**
  - A source of 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 resolve the vulnerabilities they prevent
- **This topic will explore 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
  - We will begin with the technical low-level part
    - And show the path up to the much more abstract security management techniques

Compliance as code

José Manuel
Redondo López

- **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 at scale
- **Therefore, it is the codification of our compliance controls**
  - So their adherence, application and remediation can be automated
  - This can be applied 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 (DSLs)**
  - We are software engineers! Programming languages are our bread and butter!

From security controls to methodologies

José Manuel
Redondo López

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

Managed by

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

Map to

3 Use **Implementation Groups** (only 3) to implement only the most adequate **CIS CSC Subcontrols** to my particular scenario

Can be distributed into

2 Group the implemented security controls in **CIS Critical Security Controls (CSC)** (20) and **subcontrols** (170 maximum, normally far less)

Can be grouped into

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

Spanish Esquema Nacional de Seguridad (ENS)

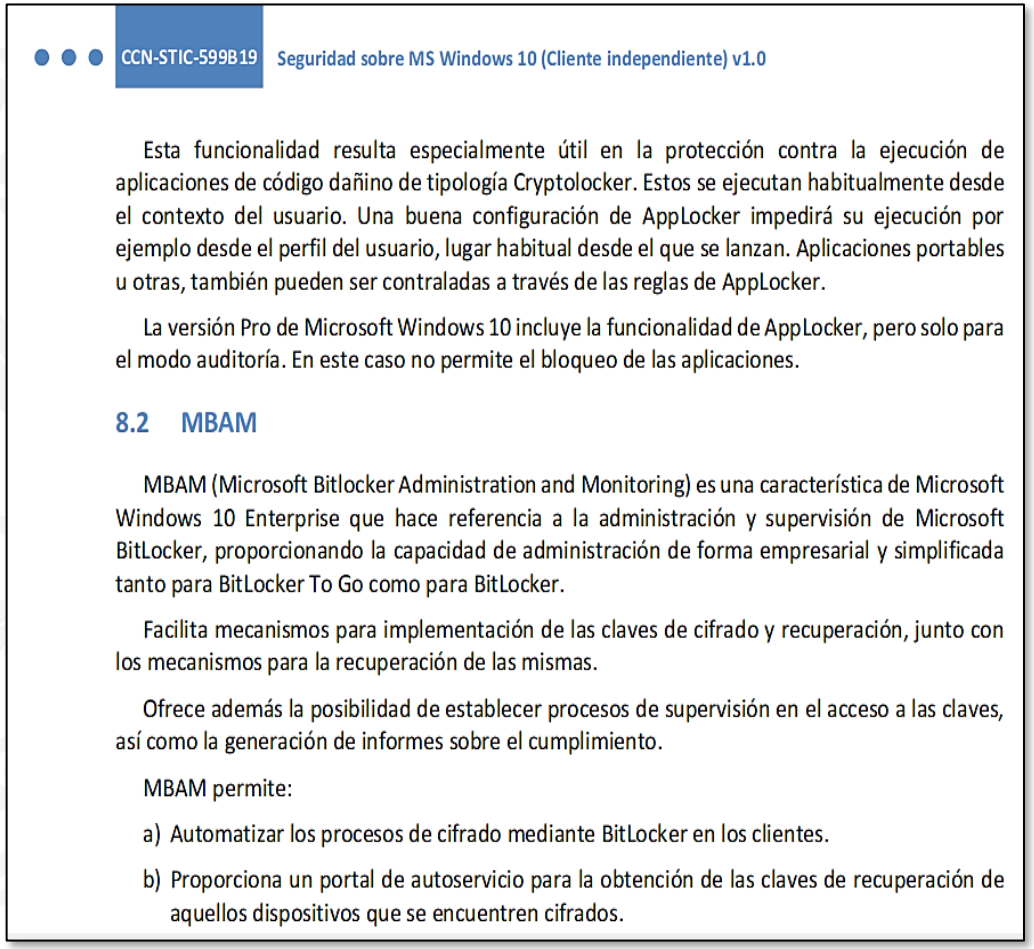
Our country's security controls

Law 11/2007 (22th June): citizens electronic access to public services: Esquema Nacional de Seguridad (Spain)

José Manuel Redondo López

- **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**
  - So they achieve ENS compliance,
  - The CCN-STIC publish free security guides for many products
    - They have lists of security controls with detailed explanations
  - Guides are organized in series. Examples:
    - **Windows** (series 500): https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/500-guias-de-entornos-windows.html
    - **Other OS** (series 600): https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/600-guias-de-otros-entornos.html
    - **Software** (series 800): https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/800-guia-esquema-nacional-de-seguridad.html

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



CCN-STIC-599B19 Seguridad sobre MS Windows 10 (Cliente independiente) v1.0

Esta funcionalidad resulta especialmente útil en la protección contra la ejecución de aplicaciones de código dañino de tipología Cryptolocker. Estos se ejecutan habitualmente desde el contexto del usuario. Una buena configuración de AppLocker impedirá su ejecución por ejemplo desde el perfil del usuario, lugar habitual desde el que se lanzan. Aplicaciones portables u otras, también pueden ser contraladas a través de las reglas de AppLocker.

La versión Pro de Microsoft Windows 10 incluye la funcionalidad de AppLocker, pero solo para el modo auditoría. En este caso no permite el bloqueo de las aplicaciones.

8.2 MBAM

MBAM (Microsoft Bitlocker Administration and Monitoring) es una característica de Microsoft Windows 10 Enterprise que hace referencia a la administración y supervisión de Microsoft BitLocker, proporcionando la capacidad de administración de forma empresarial y simplificada tanto para BitLocker To Go como para BitLocker.

Facilita mecanismos para implementación de las claves de cifrado y recuperación, junto con los mecanismos para la recuperación de las mismas.

Ofrece además la posibilidad de establecer procesos de supervisión en el acceso a las claves, así como la generación de informes sobre el cumplimiento.

MBAM permite:

a) Automatizar los procesos de cifrado mediante BitLocker en los clientes.

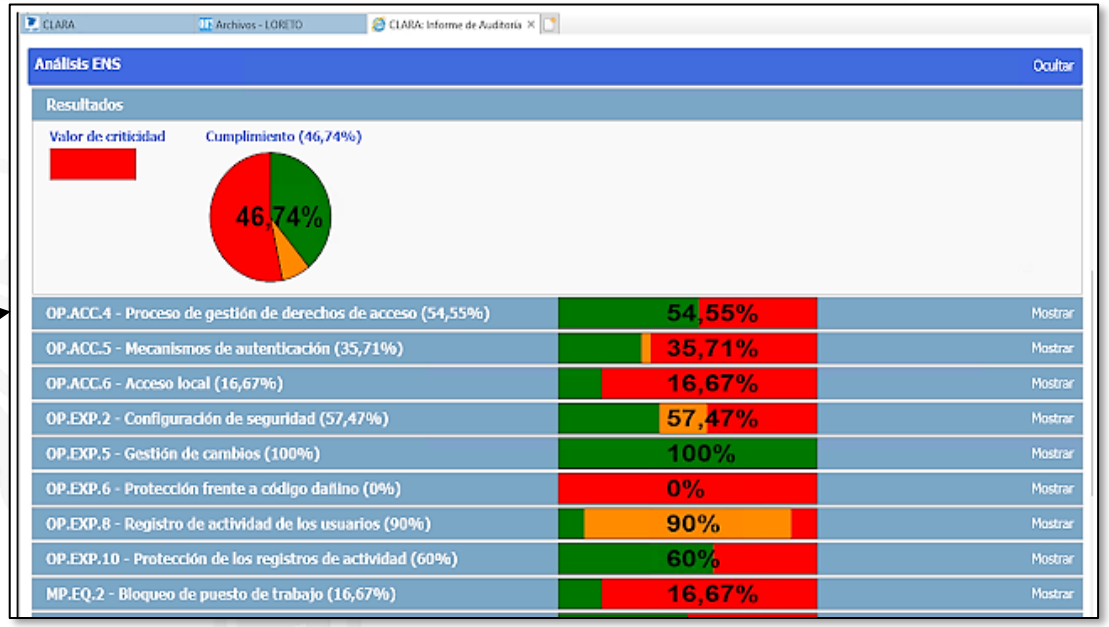
b) Proporciona un portal de autoservicio para la obtención de las claves de recuperación de aquellos dispositivos que se encuentren cifrados.

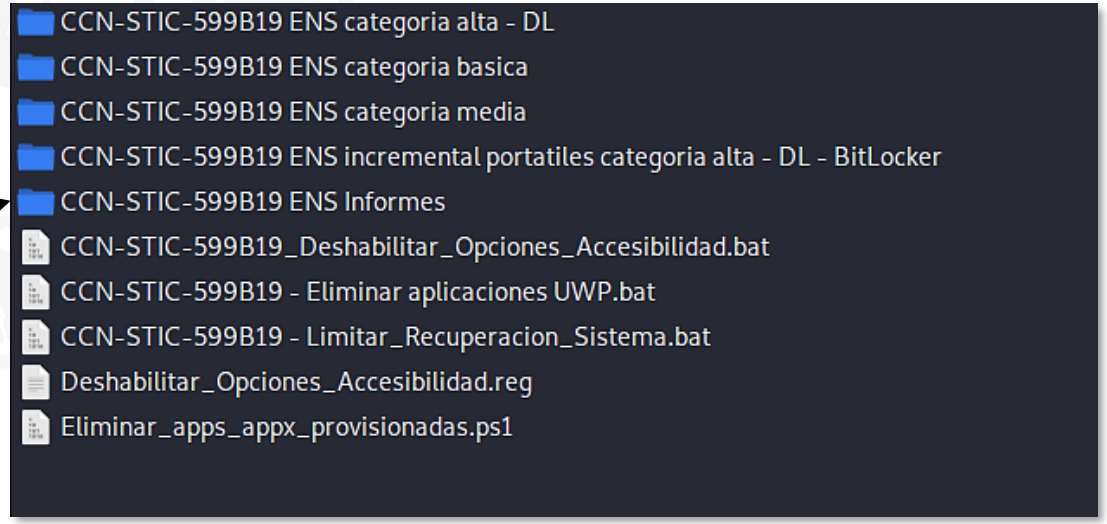
Source: https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/4095-ccn-stic-599b19-configuracion-segura-de-windows-10-cliente-independiente.html

Law 11/2007 (22th June): citizens electronic access to public services: Spanish Esquema nacional de Seguridad

José Manuel Redondo López

- **CCN-CERT also offers a series of security software available to partners**
  - 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 it does not facilitate compliance as code**
  - They are not structured as other solutions
    - Problem - description - how to check - how to remediate
    - Some lack of detailed technical procedures
  - Automated remediation measures are custom scripts
    - While very useful, they do not follow international security automation standards (SCAP, shown later)
    - The image shows these for Windows Server 2016





Security Content Automation Protocol (SCAP)

Standardized automation protocol for hardening operations that facilitate Compliance as Code

Security Content Automation Protocol (SCAP)

José Manuel
Redondo López

- **Protocol that allows automated hardening on software systems**
  - Standardized by NIST
  - SCAP-compatible tools load files built in two XML-based markup language formats
    - **OVAL and XCCDF**
  - These files are used to automate
    - Security control **evaluation** (see if the control is already applied)
    - And also, **remediation** (apply the security control to solve the associated vulnerabilities)
- **The OpenSCAP project is its most popular implementation**
  - A set of open-source tools complying with the SCAP 1.2 standard: https://www.open-scap.org/
  - These tools allow
    - Automated configuration, checking for vulnerabilities, and patches
    - Technical security control compliance activities
    - Measuring the current security level

AUTOMATED HARDENING LANGUAGES

José Manuel
Redondo López

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

```
<?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

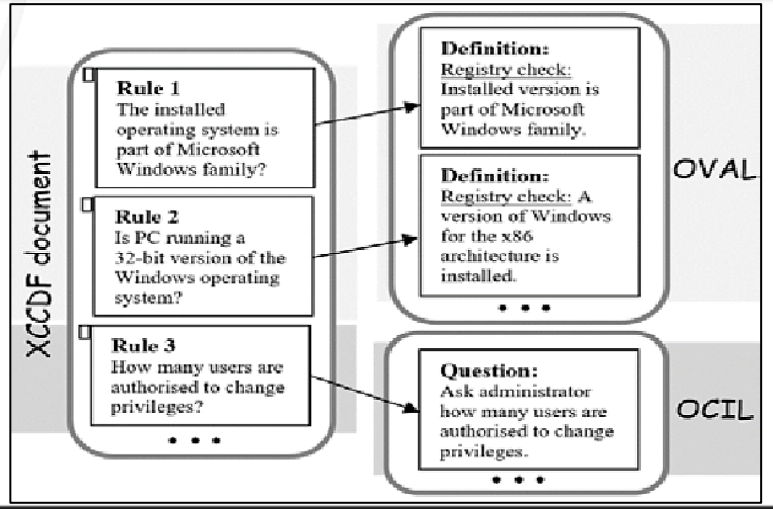
```
  <objects>
    <registry_object id="oval:jp.jvn.jvndb.oval:obj:1111"
    version="1" xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows">
      <hive>HKEY_LOCAL_MACHINE</hive>
      <key>SOFTWARE¥IPA¥MyJVN</key>
      <name>CurrentVersion<name />
    </registry_object>
  </objects>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

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>
```

- **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…)
  - Finally, it allows to create a report with the evaluation results

- **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

José Manuel Redondo López

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
  - To define a compliance policy expressed by an XCCDF checklist
- It also contains an index and catalog
  - That allow splitting the given data stream into files according to the SCAP components
- It is also an XML-based language to create a table of contents of the contained files
  - These files contain multiple components of the same type
  - Covering all security policies needed an organization
- For this reason, 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)

José Manuel
Redondo López

- **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)
- **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/

CURRENT STATE OF SECURITY AUTOMATION

José Manuel
Redondo López

- **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**
  - 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 and validated SCAP-compatible security control lists for free for all popular software and OS**

< Go to Index

Source: zona-militar.com

SCAP Sec. Guide >

STIGs >

CIS Benchmarks >

SOURCES OF VALIDATED SECURITY CONTROL LISTS

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

OpenSCAP: Choosing a policy

José Manuel
Redondo López

- **There are various sources of security policies**
- **For any possible software / OS we want to secure**
  - https://www.open-scap.org/security-policies/choosing-policy/
  - **We are going to review three of them**
  - This way, you don't need to be an expert to deploy a policy
    - Or know anything about the SCAP standard to write one
  - There are many already available in a standardized form!
  - Private infrastructures can be made compliant with any government / company / institution policy easier this way
    - So they can apply for public contracts!
- **If new policies are required, they are rarely created from scratch**
  - But created from existing ones
  - They are used as starting points, and modified to suit an organization requirements

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

The easiest to find free security control source

THE SCAP-SECURITY-GUIDE PACKAGE

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

José Manuel
Redondo López

- **The free and open SCAP tool should be also partnered with free and open files required to secure software systems**
  - Otherwise, it will not do anything!
- **The SCAP security guide package covers this requirement, containing**
  - **The `oscap` tool** (the OpenSCAP implementation)
  - **A set of SCAP-compatible preconstructed security policies**
    - Covering several security areas of different versions of software products / OS (Red Hat, Fedora, Ubuntu,…)
    - Using these files, we can attain substantially higher security levels than default installations with little effort
    - Not every security control contained in these files can be remediated using OpenSCAP (yet)
      - But alternatives are provided to try to overcome some limitations
      - 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…)

THE THE SCAP-SECURITY-GUIDE PACKAGE

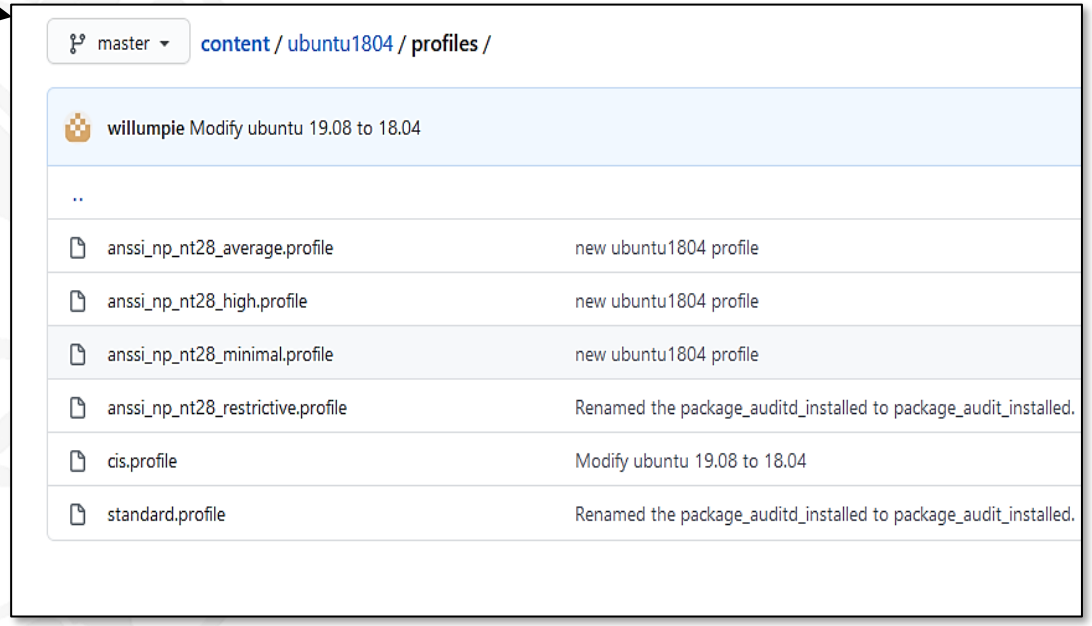
José Manuel
Redondo López

- **You new to keep the security policies of this package updated because…**
  - https://github.com/ComplianceAsCode/content
  - Support for automated security control validation and remediation of **more types of software / OS**
  - Support for **enhanced control lists**
    - Solving bugs, adding more security controls, make more security controls automatically remediable…
  - Support for **alternative remediation procedures**: If the policy lacks OpenSCAP compatible content to perform automatic remediation, sometimes these alternatives are supported
    - **Ansible content**: Ansible playbooks (sets of directories and `.yml` files)
      - Ansible is an automatic infrastructure configuration tool
        - And can be used to secure multiple machines in the same operation!
      - These can be used to evaluate compliance (check), as well as to put machines into compliance (remediate)
    - **Bash fix files**: bash scripts meant to be run on machines to put them into compliance

THE SCAP-SECURITY-GUIDE PACKAGE

José Manuel
Redondo López

- **The image shows the security profiles available in the SCAP security guide package GitHub repository 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)
- **Normally, there are no content for the most recent OS/software releases**
  - They take time to develop
  - If using a recent OS released version, updating the package frequently is even more important



THE SCAP-SECURITY-GUIDE PACKAGE

José Manuel
Redondo López

- **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
- **As we said, automatic remediation is not available or complete sometimes…**
  - Ansible or Bash content could be included to replace or complement SCAP automatic remediation
  - The image shows an Ubuntu bash remediation script
    - Supplied with the SCAP security guide package
  - These scripts can be also used to harden systems that do not have the `oscap` package installed!
- **The Ubuntu Pro license also include SCAP-compatible remediation files**
  - But following the CIS security controls we will review

```
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!
Remediating rule 37/45: 'sysctl_fs_protected_hardlinks'
FIX FOR THIS RULE 'sysctl_fs_protected_hardlinks' IS MISSING!
Remediating rule 38/45: 'sysctl_fs_protected_symlinks'
FIX FOR THIS RULE 'sysctl_fs_protected_symlinks' IS MISSING!
Remediating rule 39/45: 'sysctl_fs_suid_dumpable'
FIX FOR THIS RULE 'sysctl_fs_suid_dumpable' IS MISSING!
Remediating rule 40/45: 'sysctl_kernel_randomize_va_space'
FIX FOR THIS RULE 'sysctl_kernel_randomize_va_space' IS MISSING!
Remediating rule 41/45: 'partition_for_home'
FIX FOR THIS RULE 'partition_for_home' IS MISSING!
Remediating rule 42/45: 'partition_for_tmp'
FIX FOR THIS RULE 'partition_for_tmp' IS MISSING!
Remediating rule 43/45: 'partition_for_var'
FIX FOR THIS RULE 'partition_for_var' IS MISSING!
Remediating rule 44/45: 'partition_for_var_log'
FIX FOR THIS RULE 'partition_for_var_log' IS MISSING!
Remediating rule 45/45: 'partition_for_var_log_audit'
FIX FOR THIS RULE 'partition_for_var_log_audit' IS MISSING!
operario@server1804:/etc/oscap/content/bash$ sudo bash ubuntu1804-script-standard.sh
```

Advantages / disadvantages

José Manuel
Redondo López

- **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
  - Include a selection of security controls from other validated sources, combining them
  - Easily updatable
- **Disadvantages**
  - Incomplete for some products, or remediation is not fully available
  - 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

Security Technical Implementation Guides (STIGs)

Security control lists to make your system great again ☺

National Institute of Standards and Technology (NIST)

https://www.nist.gov/

José Manuel
Redondo López

- **Agency of the U.S. Department of Commerce**
  - Free and public **STIG archive**: **560+ security benchmarks (security control lists) for many products**
    - 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 Technical Guide to Information Security Testing and Assessment (SP 800-115)**
  - Assist organizations in planning and conducting technical information 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

José Manuel
Redondo López

- **These are applied to security controls**
- **For each type of device or application, a STIG contains hundreds of checks to determine if they meet the 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 checks in a STIG is assigned a severity level**
  - **CAT I**: Any vulnerability whose exploitation directly causes a loss of confidentiality, availability or integrity (**very serious**)
  - **CAT II**: Any vulnerability whose exploitation can potentially cause a loss of confidentiality, availability or integrity (**intermediate**)
  - **CAT III**: Any vulnerability whose exploitation causes a degradation of measures that prevent loss of confidentiality, availability or integrity (**less severe**)

Mission Assurance Category (MACs) levels

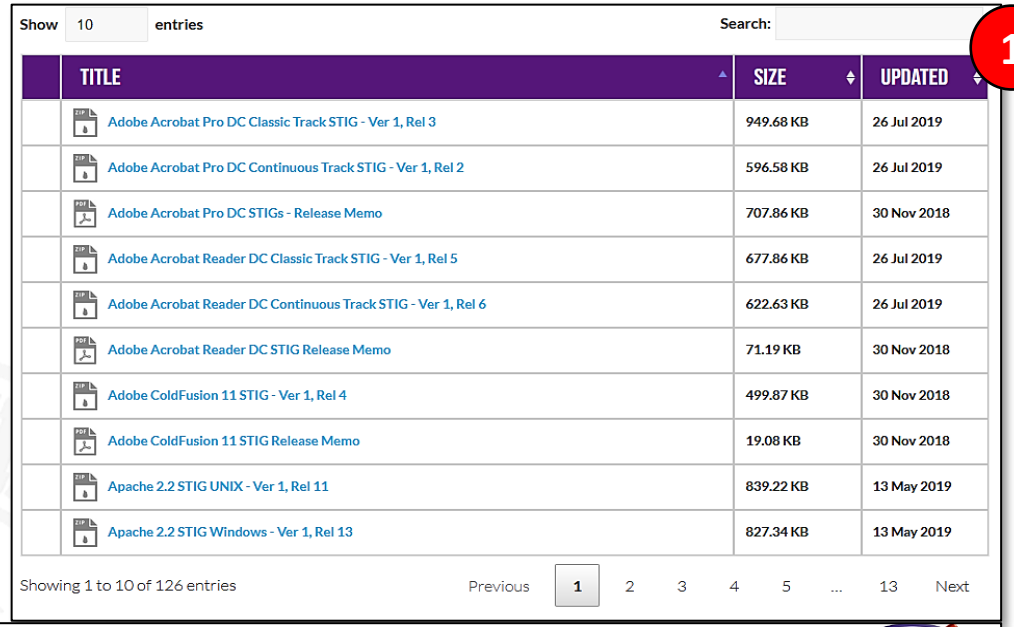
José Manuel
Redondo López

- **These are applied to machines / systems**
- **All systems within STIGs are also classified based on the importance of the information they manage, and how critical it is**
  - **MAC I**: Systems managing vital information for the effectiveness of its functionality
    - Losing one is unacceptable, **strongest security measures**
  - **MAC II**: Systems managing important information for the performed functionality
    - Losing one is a major problem, **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, security 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

José Manuel
Redondo López

- **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
  - Many can also be found in the SCAP Security Guide package we saw

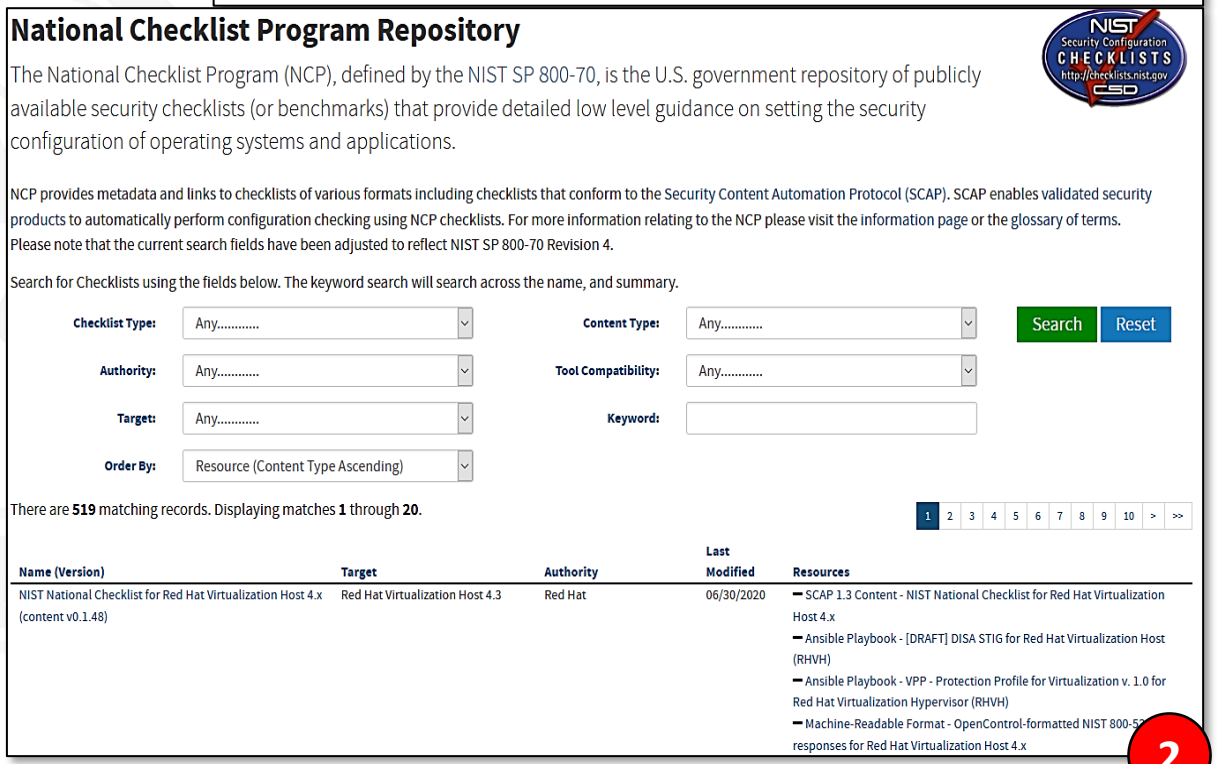


Show 10 entries Search:

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 800-5 responses for Red Hat Virtualization Host 4.x

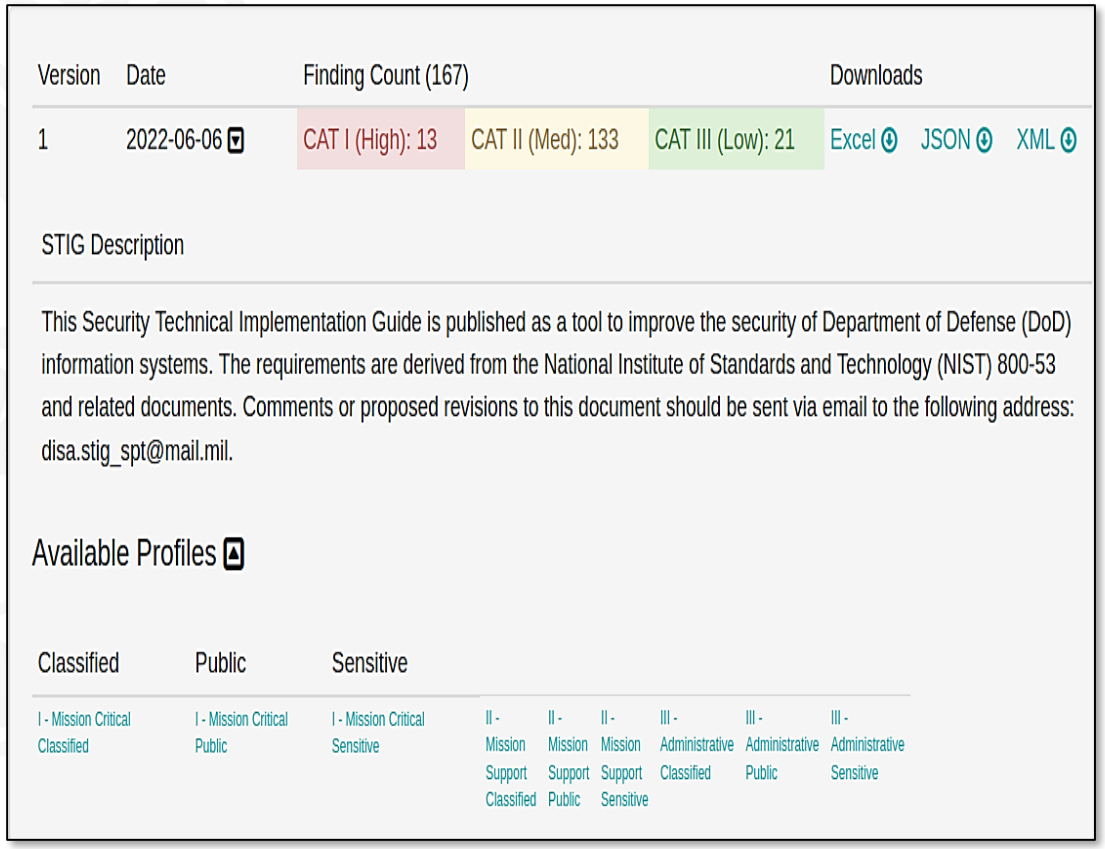
2

Example: STIG "Canonical Ubuntu 20.04 LTS": Profiles

José Manuel
Redondo López

- **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 tests 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**
  - Excel file to facilitate **manual checks**

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



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

José Manuel Redondo López

- **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 target system
  - **Title**: Summary of test objectives
  - **Description**: More detailed description of the effects or particularities of the test
- **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

José Manuel Redondo López

- **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

José Manuel
Redondo López

Advantages

- Validated security guides are available for a **wide range of products**
- These are **highly secure** (military-grade) and **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
- The **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, **not public**
    - https://www.public.navy.mil/navwar/Atlantic/Technology/Pages/SCAP.aspx
- Therefore, we need to rely in third-party automated implementations of the STIG guides
  - Like the one provided in Ubuntu Pro!
  - Or maybe develop our own automation scripts, or use the guidance for **manual checking only**
  - **However, some of them have public Ansible automated remediation procedures freely available!**

Center for Internet Security (CIS) Benchmarks

"Top Gun" security controls

CIS BENCHMARKS

https://www.cisecurity.org/

José Manuel
Redondo López

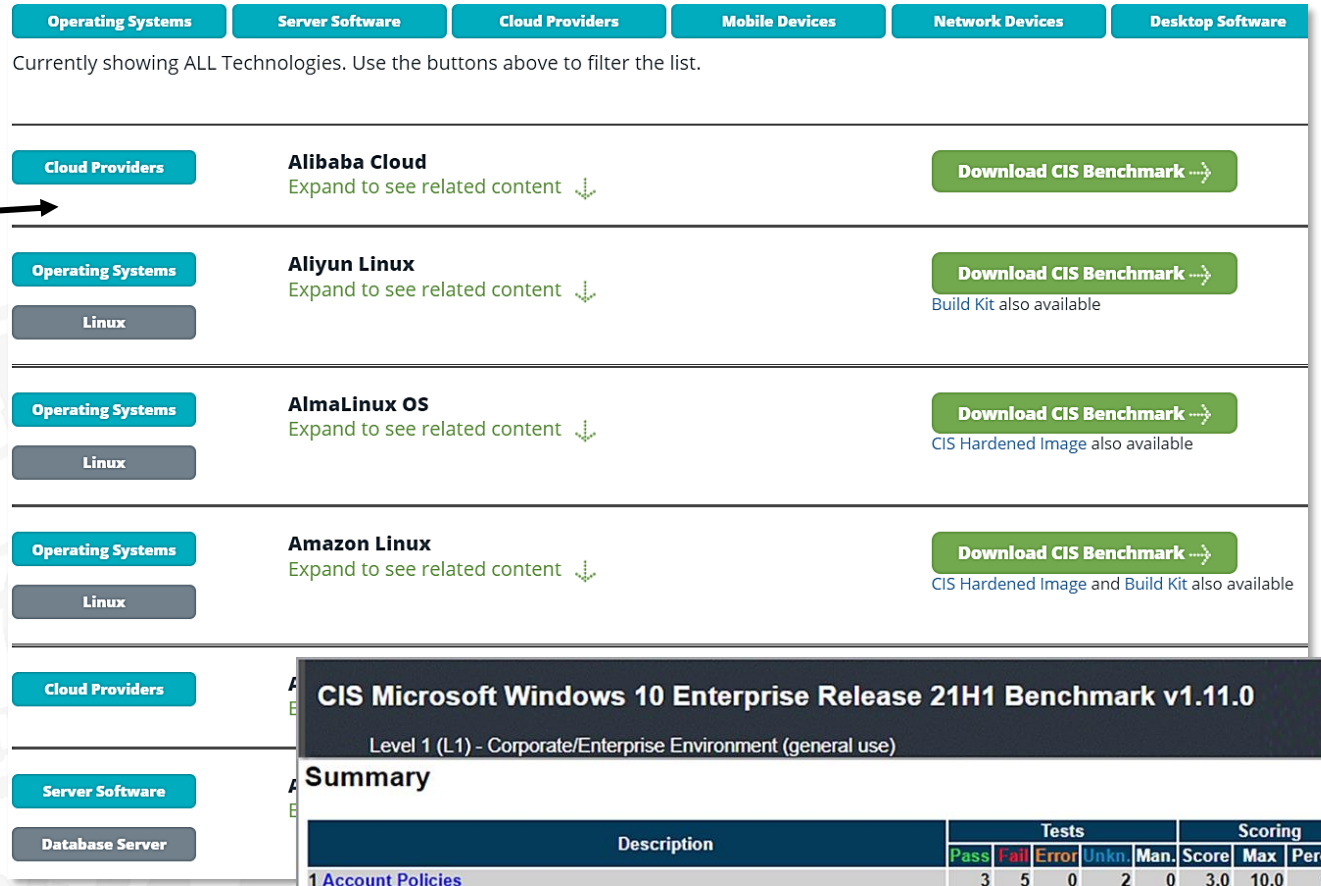
- **Well established source of hardening guides**
  - Recommend values and technical **security controls** applicable to network devices, OS, software...
  - One guide per product and version
  - Currently more than 100 are available: https://www.cisecurity.org/cis-benchmarks/
- **They are created and 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
    - Acquired from several major private **civilian companies** and public institutions worldwide
- **Apart from guides, they include (at a cost)**
  - **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

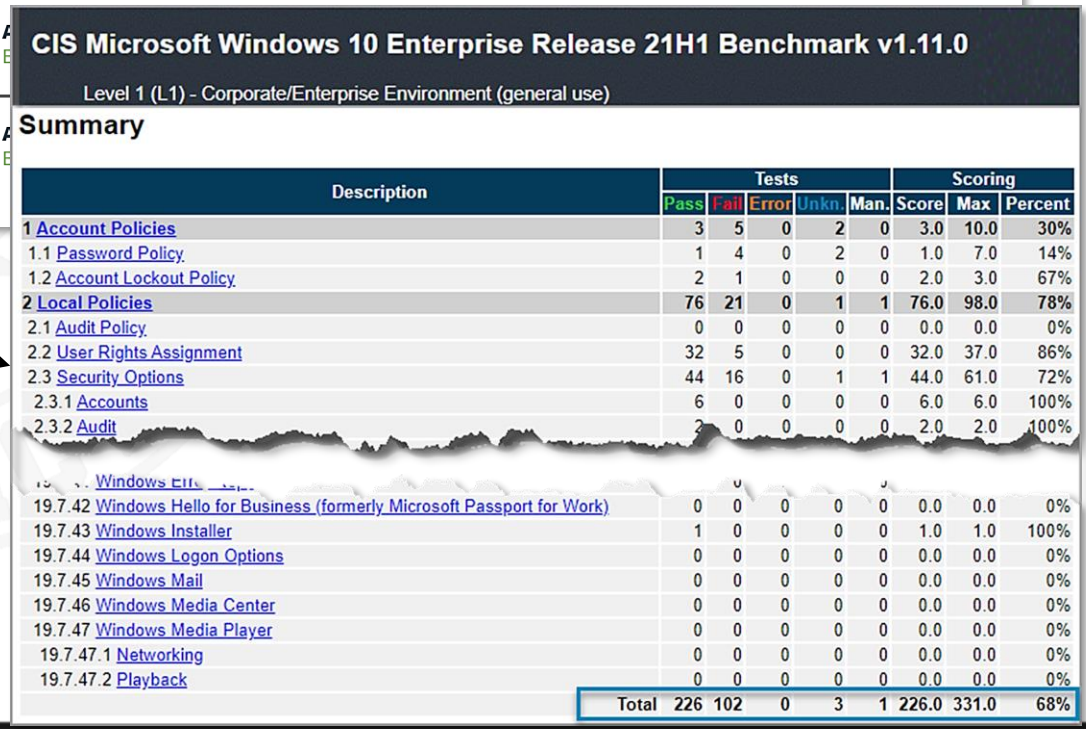
CIS BENCHMARKS

José Manuel
Redondo López

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

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





Why use CIS Benchmarks?

José Manuel
Redondo López

- **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
- **Endorsement of your work as a security engineer**
  - **The security of a system can be evaluated and expressed with a score**
  - You can measure and compare against others

CIS Benchmarks security control structure: Scoring

José Manuel
Redondo López

- **Indicates if complying with the associated control has an impact on a security score**
  - An audited system will get a score as a result
  - Scores are calculated per benchmark category and aggregated at the end
  - See the image of CIS-CAT Lite to see an example
  - **Scored**: The security control affects the score
    - If it is met, increases it
    - If not, decreases it
  - **Not Scored**: The score does not change whether the security control is fulfilled or not
    - **It is a recommendation that should be considered**
    - Desirable, but not critical

1.1.2 Ensure separate partition exists for /tmp (Scored)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The `/tmp` directory is a world-writable directory used for temporary storage by all users and some applications.

Rationale:

Since the `/tmp` directory is intended to be world-writable, there is a risk of resource exhaustion if it is not bound to a separate partition. In addition, making `/tmp` its own file system allows an administrator to set the `noexec` option on the mount, making `/tmp` useless for an attacker to install executable code. It would also prevent an attacker from establishing a hardlink to a system `setuid` program and wait for it to be updated. Once the program was updated, the hardlink would be broken and the attacker would have his own copy of the program. If the program happened to have a security vulnerability, the attacker could continue to exploit the known flaw.

Audit:

Run the following command and verify output shows `/tmp` is mounted:

```
# mount | grep /tmp
tmpfs on /tmp type tmpfs (rw,nosuid,nodev,noexec,relatime)
```

Remediation:

For new installations, during installation create a custom partition setup and specify a separate partition for `/tmp`.
For systems that were previously installed, create a new partition and configure `/etc/fstab` as appropriate.

Source: Ubuntu 18.04 Benchmark PDF file

CIS Benchmarks security control structure: Scoring

José Manuel
Redondo López

- **How many security controls exist? How many have an scored / not scored nature?**
- **It all depends on the product covered by the CIS benchmark! E. g.:**
  - The Ubuntu 18.04 CIS Benchmark has a total 241 security controls
    - 214 are scored and 27 are not
  - The Windows Server 2019 CIS Benchmark has 384 security controls
    - And all of them are scored (all are important!)
  - …
- **Different product, different security control amount and distribution**
  - CIS Benchmarks adapt to the product

CIS Benchmarks security control structure: Profile applicability

José Manuel
Redondo López

- **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
      - Provide a substantial security advantage
      - Keep the functionality of the product operative within acceptable limits
    - **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 product 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: Profile applicability

José Manuel
Redondo López

- **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

1.1.2 Ensure separate partition exists for /tmp (Scored)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The `/tmp` directory is a world-writable directory used for temporary storage by all users and some applications.

Rationale:

Since the `/tmp` directory is intended to be world-writable, there is a risk of resource exhaustion if it is not bound to a separate partition. In addition, making `/tmp` its own file system allows an administrator to set the `noexec` option on the mount, making `/tmp` useless for an attacker to install executable code. It would also prevent an attacker from establishing a hardlink to a system `setuid` program and wait for it to be updated. Once the program was updated, the hardlink would be broken and the attacker would have his own copy of the program. If the program happened to have a security vulnerability, the attacker could continue to exploit the known flaw.

Audit:

Run the following command and verify output shows `/tmp` is mounted:

```
# mount | grep /tmp
tmpfs on /tmp type tmpfs (rw,nosuid,nodev,noexec,relatime)
```

Remediation:

For new installations, during installation create a custom partition setup and specify a separate partition for `/tmp`.
For systems that were previously installed, create a new partition and configure `/etc/fstab` as appropriate.

Source: Ubuntu 18.04 Benchmark PDF file

CIS Benchmarks security control structure: Technical data

José Manuel
Redondo López

- **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 18.04 Benchmark PDF file

1.1.2 Ensure separate partition exists for /tmp (Scored)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The `/tmp` directory is a world-writable directory used for temporary storage by all users and some applications.

Rationale:

Since the `/tmp` directory is intended to be world-writable, there is a risk of resource exhaustion if it is not bound to a separate partition. In addition, making `/tmp` its own file system allows an administrator to set the `noexec` option on the mount, making `/tmp` useless for an attacker to install executable code. It would also prevent an attacker from establishing a hardlink to a system `setuid` program and wait for it to be updated. Once the program was updated, the hardlink would be broken and the attacker would have his own copy of the program. If the program happened to have a security vulnerability, the attacker could continue to exploit the known flaw.

Audit:

Run the following command and verify output shows `/tmp` is mounted:

```
# mount | grep /tmp
tmpfs on /tmp type tmpfs (rw,nosuid,nodev,noexec,relatime)
```

Remediation:

For new installations, during installation create a custom partition setup and specify a separate partition for `/tmp`.
For systems that were previously installed, create a new partition and configure `/etc/fstab` as appropriate.

CIS and Ubuntu Pro

José Manuel
Redondo López

- **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
    - That includes **automated Ubuntu Pro CIS Compliance**!
    - This enables you to automatically harden Ubuntu machines following CIS or STIG security controls
      - https://ubuntu.com/tutorials/comply-with-cis-or-disa-stig-on-ubuntu#1-overview
      - https://ubuntu.com/security/certifications/docs/cis
    - Free for up to 5 Ubuntu 18.04LTS or 20.04LTS machines
    - 22.04 is not yet supported!
- **Yes, you can now officially create bullet-proof Ubuntu machines automatically! ☺**

Advantages / disadvantages

José Manuel
Redondo López

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
- Best official tools to automate their security control verification and application are not free
  - The free Lite version only supports Windows 10, Ubuntu, and Chrome: https://learn.cisecurity.org/cis-cat-lite
  - Or we must rely on **unofficial tools to automate its verification / application**
  - **Or just trust that the current OpenSCAP support for CIS benchmarks will substantially improve**
- Being so extensive, adapting them to a specific functionality can be tedious

And what happens with Windows® systems?

José Manuel
Redondo López

- **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 access
  - Our student María Flórez implemented this as her final degree project
    - https://github.com/Yori1999/vagrant-ansible-hardening
- **Microsoft also publishes their own security baselines (security controls to implement) and automation software**
  - Hence, Microsoft has their own standard to do this
  - https://learn.microsoft.com/es-es/windows/security/threat-protection/windows-security-configuration-framework/windows-security-baselines

< Go to Index

Security frameworks: Towards a higher level of abstraction

Using technical security controls to create security policies

Source: zona-militar.com

From security controls to methodologies

José Manuel
Redondo López

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

Managed by

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

Map to

3 Use **Implementation Groups** (only 3) to implement only the most adequate **CIS CSC Subcontrols** to my particular scenario

Can be distributed into

2 **Group the implemented security controls in CIS Critical Security Controls (CSC) (20) and subcontrols (170 maximum, normally far less)**

Can be grouped into

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

BEYOND SECURITY CONTROL TECHNICAL GUIDELINES

José Manuel
Redondo López

- **Applying hundreds of validated security controls ensures 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 for the technical details** of each system
    - Focusing on "what" instead of "how" (**detailed technical information does not belong to this level**!)
    - Ideally, 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) v7

José Manuel
Redondo López

- **At the end of each technical security control of any CIS benchmark we can find which CSC Controls and CSC Subcontrols are associated with it**
  - CSC Controls represent **20** (**v7**) or **18** (**v8**) recognized best defensive cybersecurity practices
  - They are subdivided in **170 CSC subcontrols (v7)** or **153 CSC Subcontrols (v8)**
- **These 20 CSC v7 controls are also divided in 3 categories**
  - https://www.cisecurity.org/controls/cis-controls-list/
  - **Basic** (6 controls)
  - **Foundational** (10 controls)
  - **Organizational** (4 controls)

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.	●	●	●

- **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**
- **A similar mapping to Version 8 of the CSC Controls is also included: https://www.cisecurity.org/controls/v8/**

CIS Critical Security Controls (CSC controls) v7

José Manuel
Redondo López

- **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 the protections that could benefit any company
  - **Sometimes they are named just "CIS Controls"**
- **The 20 CSC v7 Controls and their associated 170 subcontrols 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

Source: https://www.cisecurity.org/insights/blog/cis-controls-version-7-whats-old-whats-new

CIS Critical Security Controls (CSC controls) v7

José Manuel
Redondo López

- **170 CSC Subcontrols are still too many entities, isn't it? Yes, but…**
  - Technical security controls of products do not map to each available CSC Control and Subcontrol!
- **Each CIS Benchmark only contain reasonable actions for their product**
  - E. g. The Google Chrome CIS Benchmark explains how to harden this browser
  - It does not have any technical security control mapping to the "Inventory and Control of Hardware Assets" CSC Control: **It is a browser, not an infrastructure!**
- **For example, the current version of the Ubuntu 18.04 CIS Benchmark has**
  - 241 technical security controls that are classified in 38 (out of 170) CSC Subcontrols v7
  - These 38 CSC Subcontrols belong to only 11 of the 20 CSC Controls v7 available
  - This way, 241 technical procedures…
    - Are grouped in 38 CSC Subcontrols
    - And these CSC Subcontrols are again grouped in only 11 CSC Controls
  - Each grouping has more abstraction level than the previous, facilitating security management
  - **38 or 11 high-level entities are easier to manage than 241 low-level ones!**

From technical security controls to CSC Controls

José Manuel
Redondo López

Ubuntu 18.04
CIS Benchmark (PDF)

CSC Controls v7
(and its CSC Subcontrols)

All technical security controls belonging to Subcontrol 4.9

All technical security controls belonging to Subcontrols 12.11 and 12.12

All technical security controls belonging to Subcontrols 16.6 and 16.8

CSC Control 4 – Controlled use of Administrative Privileges

- *4.9 Log and Alert on Unsuccessful Administrative Account Login*

CSC Control 12 – Boundary Defense

- *12.11 Require all Remote Login to Use Multi-Factor Authentication*
- *12.12 Manage All Devices Remotely Logging into Internal Network*

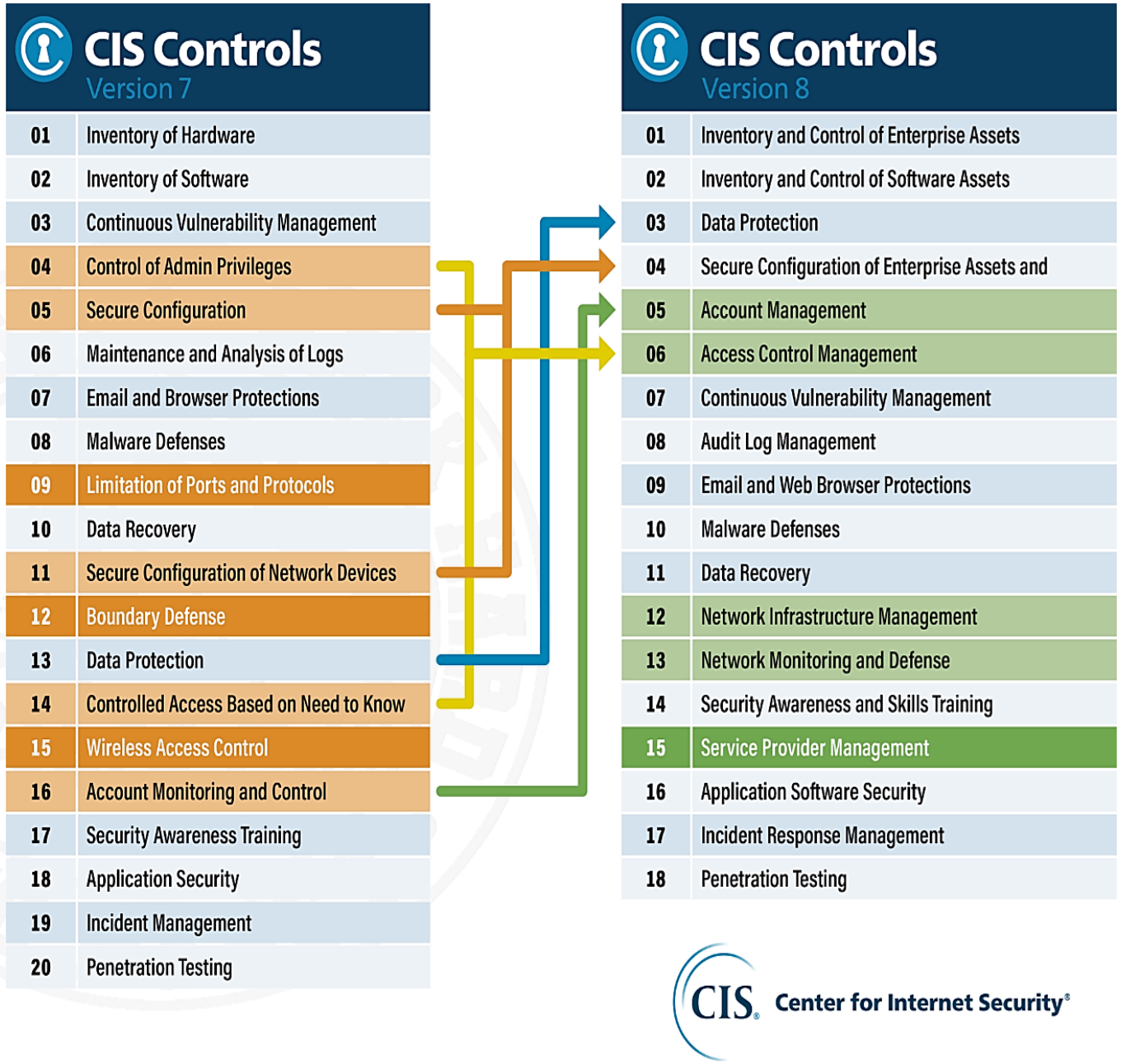
CSC Control 16 – Account Monitoring and Control

- *16.6 Maintain an Inventory of Accounts*
- *16.8 Disable Any Unassociated Accounts*

CSC Controls v8 vs v7

José Manuel
Redondo López

- **CIS Controls v8 were released in 2021**
- **They follow the same philosophy, but were updated**
  - 4 of them (light orange) have been fused in 2
    - Therefore, from 20 CSC Controls we now have 18 total
  - Some have been reformulated
  - Old ones (dark orange) have been integrated in new ones (light green)
- **Everything we said is still valid in the new version**



Source: https://www.sans.org/blog/cis-controls-v8/

From security controls to methodologies

José Manuel
Redondo López

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 subcontrols 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 **CIS CSC Subcontrols** to my particular scenario — 3

Can be distributed into

Group the implemented security controls in **CIS Critical Security Controls (CSC)** (20) and **subcontrols** (170 maximum, normally far less) — 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

Implementation groups (IGs)

José Manuel
Redondo López

- **In a previous slide about CSC Controls, you saw this…What is an IG?**
- **CSC Controls are used by companies that have a high number of resources**
  - With widely different risk exposures
  - So an efficient cybersecurity policy can be set up
- **However, in some scenarios applying CIS Controls is still 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)

José Manuel
Redondo López

- **IGs provide**
  - A new **classification / prioritization** of the CSC Subcontrols 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 CSC Subcontrols belonging to that IG
- **In other words: it narrows down how many CSC subcontrols you must implement**
  - But considering the company **perceived security risks** and **economic resources**
  - As you saw, all 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 IG you choose!**
    - In the previous table, that technical security control must be implemented, no matter the IG you chose

Implementation groups (IGs)

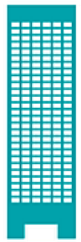
José Manuel
Redondo López

- **IGs are categories that companies may use to auto-evaluate their security**
  - Based on relevant cybersecurity attributes
  - So, each IG identifies what CSC subcontrols (and CSC Controls) are reasonable for companies with a certain risk profile and economic resources to implement security operations
  - This way, any company can easily 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
    - They provide an effective security level with already available technologies and processes
    - **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 CSC subcontrols for companies with more resources and experience, but also with a higher risk exposure than IG1 companies, must implement
  - **IG3**: incorporates the rest of CSC subcontrols not included in the previous levels
    - Maximum risk exposure and necessary economical cost, but also the maximum security level

IMPLEMENTATION GROUPS (IGS)

José Manuel
Redondo López

Source: https://www.cisecurity.org/blog/v7-1-introduces-implementation-groups-cis-controls/



Implementation Group 3
A mature organization with significant resources and cybersecurity experience to allocate to Sub-Controls

Implementation Group 2
An organization with moderate resources and cybersecurity expertise to implement Sub-Controls

Implementation Group 1
An organization with limited resources and cybersecurity expertise available to implement Sub-Controls

Definitions	1	2	3
Implementation Group 1 CIS Sub-Controls for small, commercial off-the-shelf or home office software environments where sensitivity of the data is low will typically fall under IG1. Remember, any IG1 steps should also be followed by organizations in IG2 and IG3.	●		
Implementation Group 2 CIS Sub-Controls focused on helping security teams manage sensitive client or company information fall under IG2. IG2 steps should also be followed by organizations in IG3.	●	●	
Implementation Group 3 CIS Sub-Controls that reduce the impact of zero-day attacks and targeted attacks from sophisticated adversaries typically fall into IG3. IG1 and IG2 organizations may be unable to implement all IG3 Sub-Controls.	●	●	●

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 critical data.
I will classify myself as IG1, so now I will follow only the **CIS subcontrols** of this **Implementation Group**, and implement all the related **security controls** of the **CIS Benchmark** of my **Ubuntu 18.04 + Apache** web server that are related to them

CIS, SECURITY FRAMEWORKS, AND POLICIES

José Manuel
Redondo López

- **IGs focus the cybersecurity efforts of a company in the most important areas**
  - Resource usage considering their risk is maximized
- **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/
- **There are multiple security frameworks used worldwide**
  - The following slide show some of them

CIS, SECURITY FRAMEWORKS, AND POLICIES

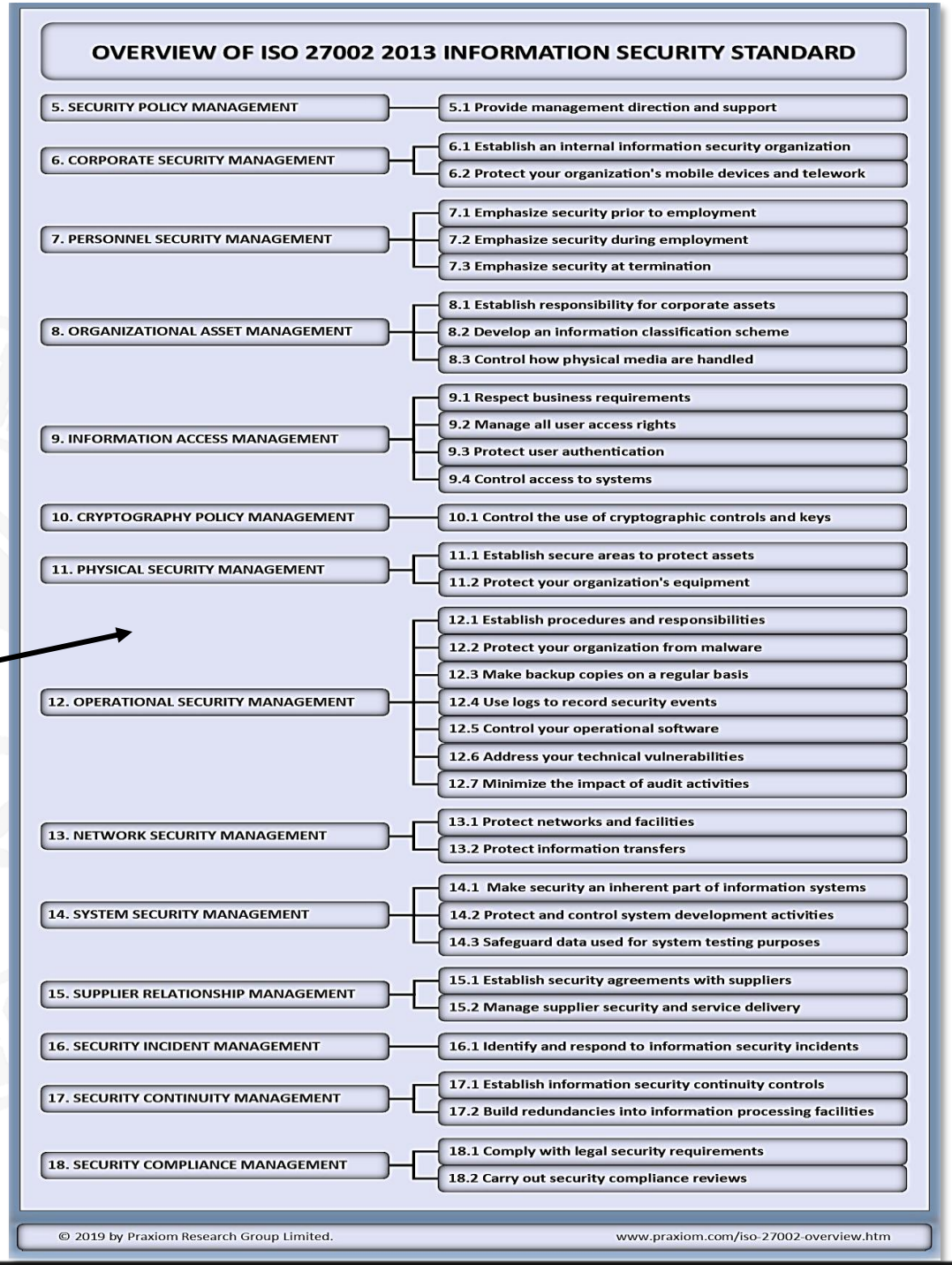
José Manuel
Redondo López

- **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
  - CIS Benchmarks and CIS controls help facilitates compliance with this framework
- **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, 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

José Manuel Redondo López

- **General Data Protection Regulation 2016/679 of the European Union**
  - CIS controls can help to achieve **GDPR compliance**
  - https://www.cisecurity.org/gdpr/
- **International Organization for Standardization (ISO) ISO/IEC 27001**
  - Provides **independent and validated worldwide standards to ensure cybersecurity**
  - It helps companies to defend against cybernetic threats and security risks
  - CIS Controls are also commonly used to achieve compliance with ISO standards

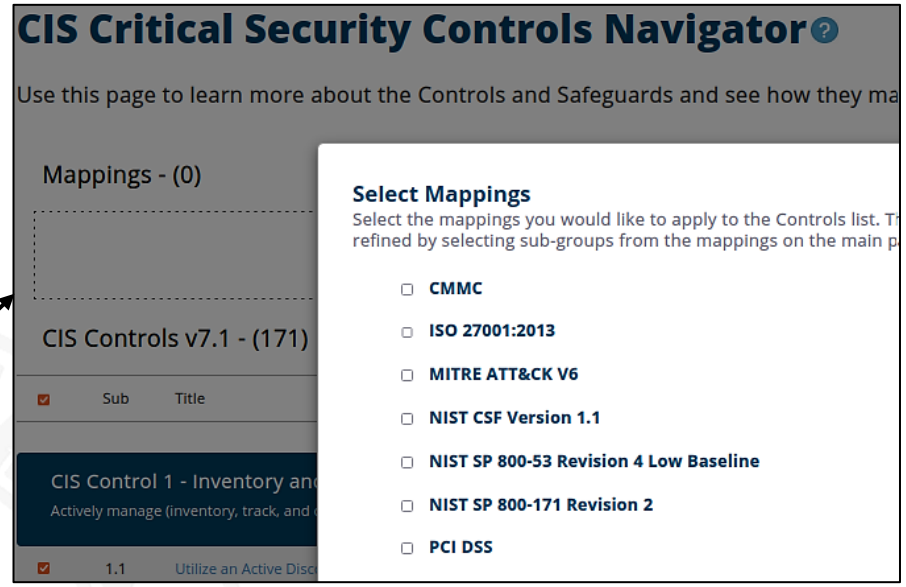


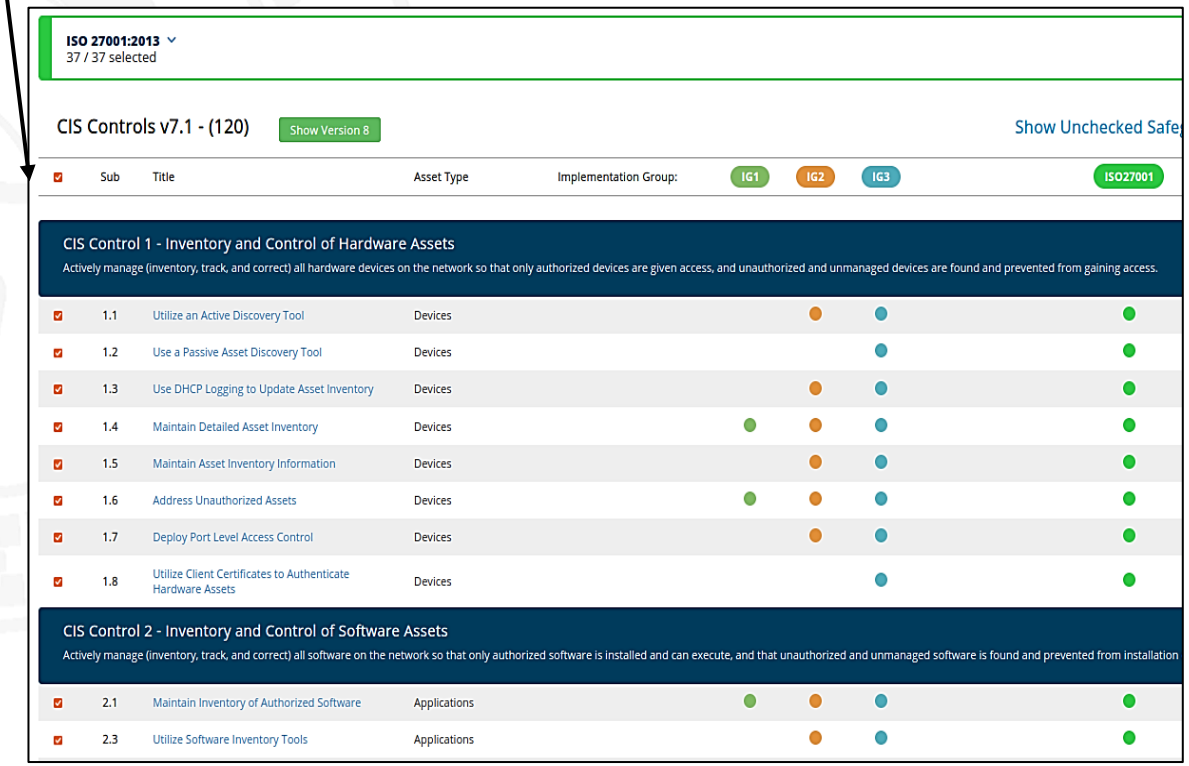
Source: https://www.praxiom.com/iso-27002-overview.htm

From CIS CSC controls to security frameworks

José Manuel Redondo López

- **CIS way to help to complying with multiple frameworks is documented**
  - CSC controls and subcontrols 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 of the OS / software they cover
  - Once implemented, you can calculate how many CIS Controls and subcontrols you are covering
  - Then, you can **map** them to a cybersecurity framework you must implement in your company
  - This way, your technical work can be translated to any of those frameworks
    - Saving time and resources!
  - So, you can now implement an ISMS easier (see next section)





CIS AND COMPLIANCE AS CODE

José Manuel
Redondo López

- **STIGs and CIS Benchmarks are related, there are mappings between the two sources of security controls**
  - https://www.cisecurity.org/blog/new-options-from-cis-for-stig-compliance/
- **There are not public known mappings between ENS and CIS Benchmarks**
  - As both can be mapped to the ISO 27001 controls, a “bridge” can be created between them
- **If you don’t have the time or resources to implement compliance, remember that you can pay for CIS-hardened images available for major cloud providers**
  - https://www.cisecurity.org/cis-hardened-image-list/
- **Microsoft has the Security Compliance Toolkit for automated compliance for Windows systems**
  - This is unrelated to CIS Benchmarks or any SCAP-compliant technology
  - It is a Microsoft-only solution
  - https://www.microsoft.com/en-us/download/details.aspx?id=55319

< Go to Index

How to implement >

Source: zona-militar.com

ISMS IMPLEMENTATION

What is an ISMS?

From security controls to methodologies

José Manuel
Redondo López

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 subcontrols 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 CIS CSC Subcontrols to my particular scenario — 3

Can be distributed into

Group the implemented security controls in **CIS Critical Security Controls (CSC)** (20) and **subcontrols** (170 maximum, normally far less) — 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

Information Security Management System (ISMS)

José Manuel
Redondo López

- **Security management must be done**
  - Through a **systematic**, **documented** and **known** process
  - **Fully accepted** company-wide (no exclusions, no matter experience, position…)
- **This management 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 information confidentiality, integrity and/or availability

ISMS ELEMENTS

José Manuel
Redondo López

- **A security policy, organization structure, procedures, processes and resources 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 risks that are beyond this risk level
  - **Documented** related policies and procedures
  - Deployed a continuous **review and improvement** process of the whole system

ISMS DEPLOYMENT ADVANTAGES

José Manuel
Redondo López

- **Reduce the risks**, following their monitoring controls
  - Threats are reduced; damage, if any, is minimized
- **Cost savings** due to resource usage optimization
  - Correct risk estimation eliminates 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
  - 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
  - If 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 admins

Spanish / European security-related law

José Manuel
Redondo López

- **Main cybercrimes can be divided in four groups**
  1. **Crimes against privacy**: illegal treatment of personal data
  2. Distribution of **illegal content**
  3. **Economic crimes**: (un)authorized access to computer systems to commit fraud, sabotage or counterfeiting
  4. **Intellectual property crimes**: protection of computer programs, databases, copyrights…
- **An ISMS can only be implemented and certified if complies the current legislation**
- **Some Spanish laws are**
  - Organic Law 15/99 on the protection of Personal Data (LOPD)
  - Law 34/2002 on Information Society Services and Electronic Commerce (LSSI)
  - General Law 32/2003 on Telecommunications
  - Law 59/2003 on Electronic Signature
  - Law 11/2007 Citizens' Electronic Access to Public Services
  - … this is the subject of **another course** (ASLEPI, 4th year)

How ISMS are implemented

ISO 27000:2013 example

ISO / IEC 27000

José Manuel
Redondo López

- **International standard set developed by**
  - The International Organization for Standardization (ISO)
  - International Electrotechnical Commission (IEC)
- **Provides an Information Security Management framework for any organization**
- **Composed by several standards, such as the ISO/IEC 27001**
  - Contains the requirements for establishing, implementing, operating, monitoring, maintaining, and improving an ISMS
  - Collects system components, the minimum documents that are part of it, the records, security controls to be implemented, and the security measures tailored to the needs of each organization
  - It describes 14 domains or areas of action, 35 control objectives or aspects to be secured within each area, and 114 controls or mechanisms to secure the objectives
  - The only one in the 27000 family that is **certifiable** once it is implemented
    - As **it is a management standard**
  - AENOR is the main Spanish certification agency
    - Asociación Española de NORmalización y Certificación: http://www.aenor.es/aenor/inicio/home/home.asp

ISO 27002

José Manuel
Redondo López

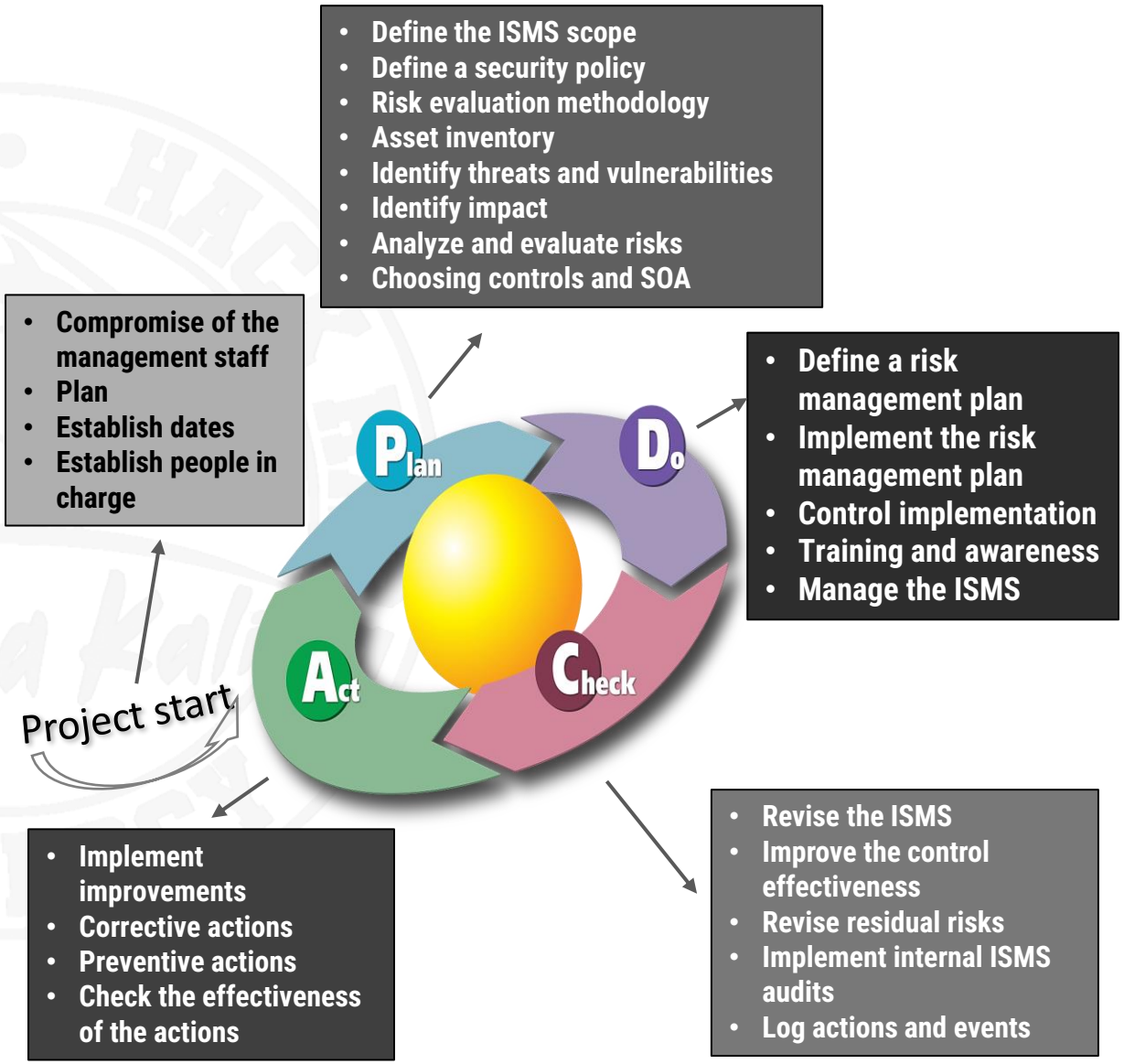
- **Detailed best practices guide / recommendations**
  - About the measures to take to secure organization's information systems
- **ISO 27002 is a supporting document to help implementing ISO 27001**
  - ISO 27001 Appendix A contains the basic overview of the security controls needed to build an Information Security Management System (ISMS)
  - ISO 27002 provides **much more detail** about the controls necessary to implement ISO 27001
    - In other words, it shares the same list 114 controls of ISO 27001, but explains each control much more
  - Essentially, **you can't meet ISO 27001 without implementing ISO 27002**
  - **But ISO 27002 is NOT a management standard**
    - It explains all the controls, no matter if a company needs them or not
    - Companies **CANNOT** be certified against ISO 27002, only ISO 27001
  - ISO 27002 is extensively used by multinational corporations and for companies that do not have to specifically comply with US federal regulations

ISMS IMPLEMENTATION STAGES (DEMING CYCLE)

José Manuel
Redondo López

- **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



PLAN: DEFINE THE ISMS BOUNDARIES

José Manuel
Redondo López

- **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

José Manuel
Redondo López

- **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

José Manuel
Redondo López

- **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 goals and limitations
  - Express support and approval from the CEO / management
  - Organization security values
  - General and particular responsibilities about how to manage information security
  - References to supporting documents

PLAN: DEFINE THE SECURITY POLICY. EXAMPLE

José Manuel
Redondo López

Objetivo:

Definir las pautas de propósito general para asegurar una adecuada protección de la información del DAPRE.
Brindar apoyo y orientación a la dirección con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y las leyes pertinentes.

Aplicabilidad:

Estas son políticas que aplican a la Alta Dirección, Ministros Consejeros, Consejeros Presidenciales, Directores, Secretarios, Jefes de Oficina, Jefes de Área, funcionarios, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales del DAPRE.

Directrices:

- Se debe verificar que se definan, implementen, revisen y actualicen las políticas de seguridad de la información.
- Diseñar, programar y realizar los programas de auditoría del sistema de gestión de seguridad de la

información, los cuales estarán a cargo de control interno.

- Todo aplicativo informático o software debe ser comprado o aprobado por el Área de Información y Sistemas en concordancia con la política de adquisición de bienes de la entidad de acuerdo con lo definido en el proceso **C-BS-07 Adquisición de Bienes y Servicios**.
- El DAPRE debe contar con un *firewall* o dispositivo de seguridad perimetral para la conexión a Internet o cuando sea inevitable para la conexión a otras redes en *outsourcing* o de terceros.
- La conexión remota a la red de área local del DAPRE debe realizarse a través de una conexión VPN segura suministrada por la entidad, la cual debe ser aprobada, registrada y auditada, a excepción de los casos que autorice el Área de Información y Sistemas.
- Los jefes de área o dependencia deben asegurarse que todos los procedimientos de seguridad de la información dentro de su área de responsabilidad, se realizan correctamente para lograr el cumplimiento de las políticas y estándares de seguridad de la información del 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

José Manuel
Redondo López

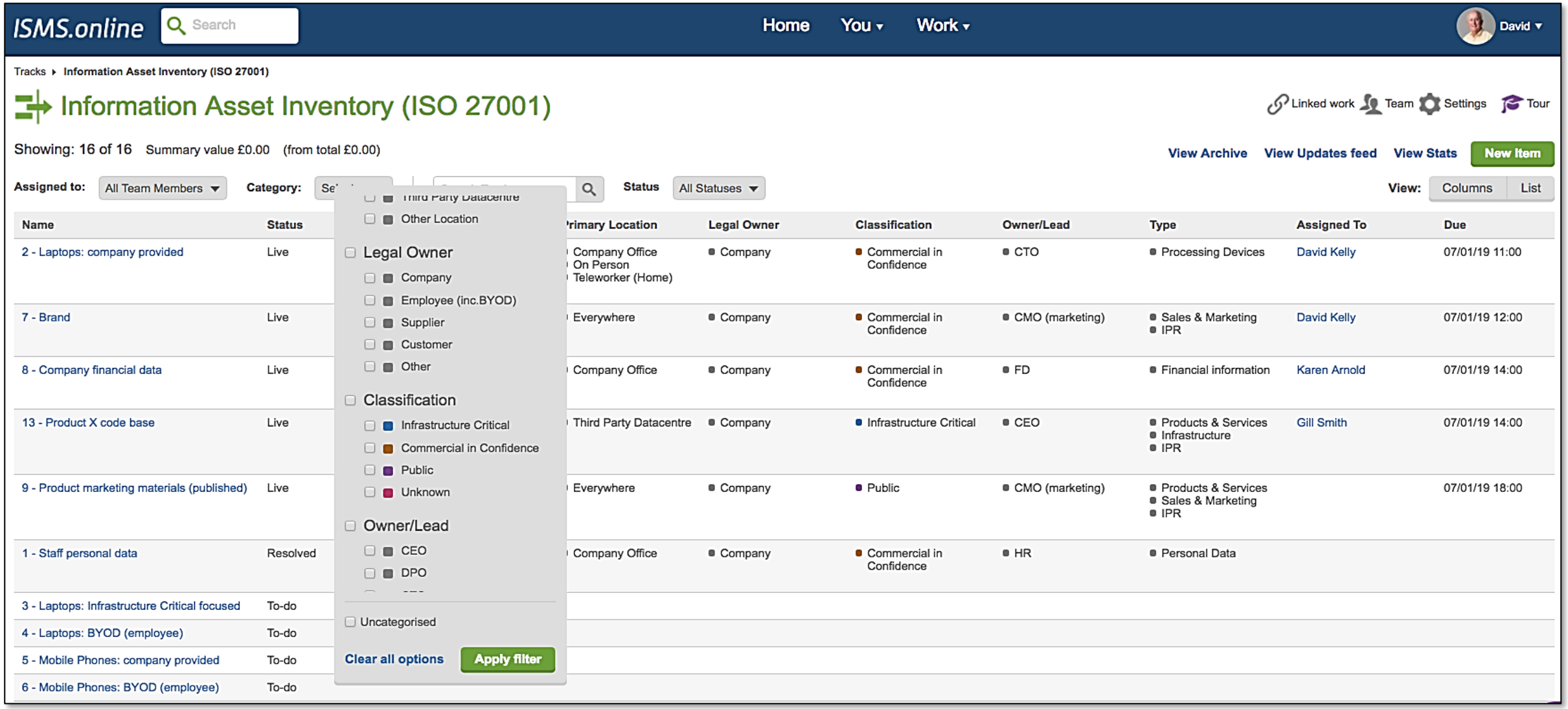
- **Assets are key resources to ensure proper operation of the organization**
- **Therefore, anything valuable enough to be protected**
  - Information
  - Buildings
  - Computer systems
  - Applications
  - Databases
  - Networks
  - Storage media
  - …
- **Asset definition must include**
  - An **inventory**: 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

José Manuel
Redondo López

- **Typical asset inventory**

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



PLAN: RISK ANALYSIS

José Manuel
Redondo López

- **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

José Manuel Redondo López

- **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 failures**,
    - 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 sensible ports evading firewall rules
	XSS due to lack of proper validation leading to scrip 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

José Manuel
Redondo López

- **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 a control to eliminate it
  - **Transfer the risk management** to an external agent
    - E. g. subcontract the service
  - **Assume** the risk
- **Finally, the residual risk must be analyzed**
  - Existing risk level after safeguards have been implemented

PLAN: DEFINE CONTROLS AND PROCEDURES

José Manuel Redondo López

- **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, that contains**
  - 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 at Clause 6 of ISO 27001. The SoA must contain at least 114 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

Legend (for Selected Controls and Reasons for controls selection)

Current as of:

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: DEFINE CONTROLS AND PROCEDURES

José Manuel Redondo López

A.5. Information security policies
These controls describe how the organization should handle its information security policies.
A.6. Organization of information security
These controls provide a framework for information security by defining the internal organization, such as roles and responsibilities, as well as other information security aspects of the organization such as the use of mobile devices, project management and even teleworking.
A.7. Human resource security
This domain presents controls that tackle the information security aspects of HR.
A.8. Asset management
These controls concern assets that are used in information security as well as designating responsibilities for their security.
A.9. Access control
These controls limit access to information assets and are both logical access controls and physical access controls.
A.10. Cryptography
This domain presents us with a proper basis for use of encryption to protect the confidentiality, authenticity and integrity of your organization's information.
A.11. Physical and environmental security
These controls are concerned with physical areas, equipment and facilities and protect against intervention, both by humans and nature.
A.12. Operations security
These controls ensure that the organization's IT systems, operating systems and software are protected.
A.13. Communications security
These are controls for the network (infrastructure and services) and the information that travels through it.
A.14. System acquisition, development and maintenance
Controls to ensure that information security is paramount when purchasing or upgrading information systems.
A.15. Supplier relationships
These controls are meant to ensure that suppliers/partners use the right Information Security controls and describe how third-party security performance should be monitored.
A.16. Information security incident management
This domain contains controls related to security incident management related to security incident handling, communication, resolution and prevention of incident reoccurrence.
A.17. Information security aspects of business continuity management
Controls to ensure information security management continuity during disruptions as well as information system availability.
A.18. Compliance
The controls in this domain are a framework to prevent legal, regulatory, statutory and breaches of contract. They also can be used to audit whether your implemented information security is effective based upon the ISO 27001 standard.

Controls and procedures can be implemented from

- CIS CSC Controls (if there is a mapping) and CIS Benchmarks (technical procedure)
- ISO 27002 contents
- Other similar information sources

Control example

A.9 Access control (area of application)

User Access control (managed entity)

User password management (security control)

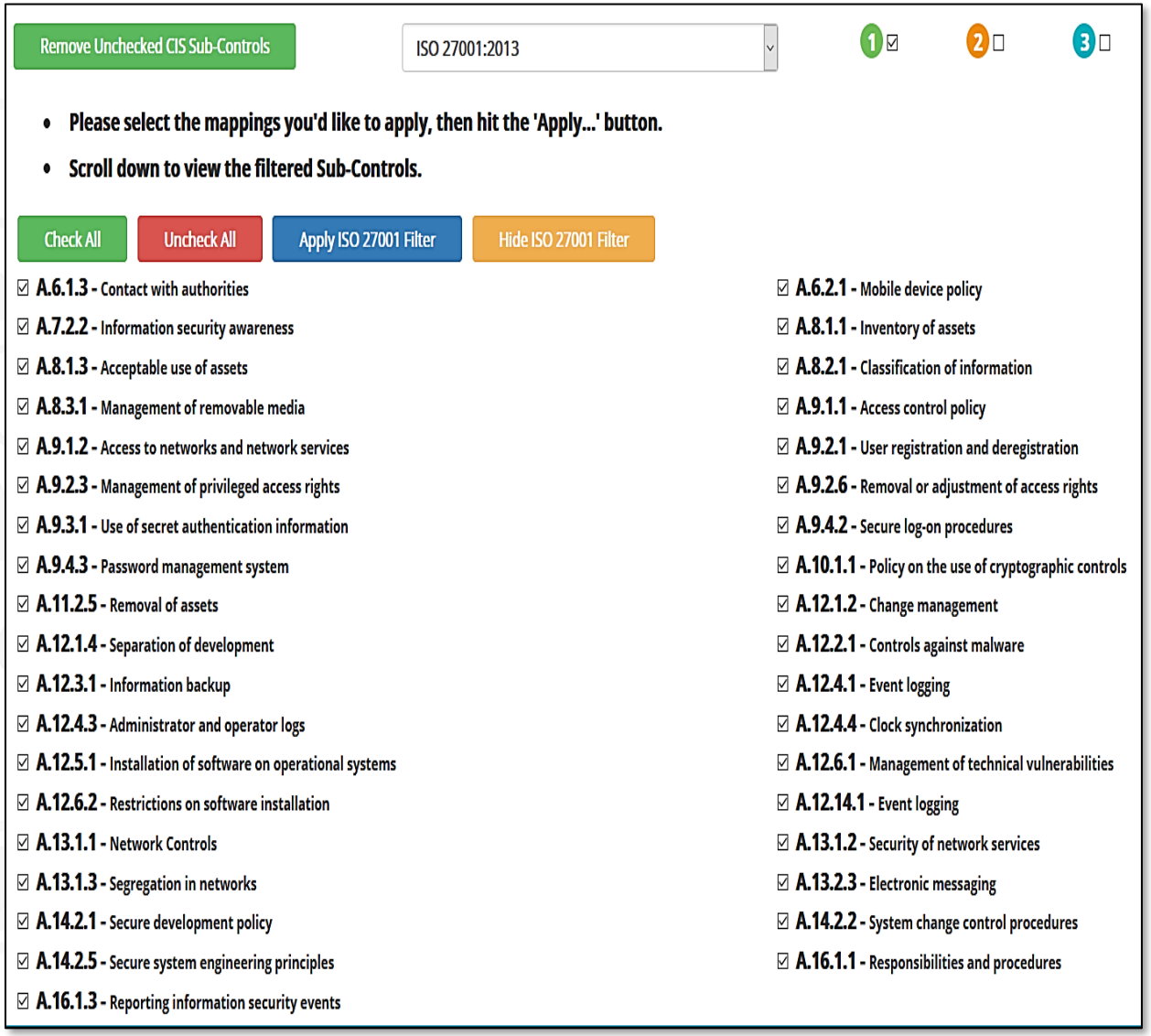
1. They must be a combination of digits, alphabetic and special characters
2. Upper and lowercase characters must be used
3. They will be changed periodically
4. Password reuse is forbidden

Source: https://resources.infosecinstitute.com/topic/iso-27001-framework-what-it-is-and-how-to-comply/

ISO 27001 CERTIFICATION

José Manuel
Redondo López

- **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
- **If we need ISO controls that cannot be mapped to CIS Controls, we can use the guidelines of the ISO 27002**
  - Current version is ISO/IEC 27701:2021
  - https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0067527



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

From CIS Benchmarks to ISO 27001:2013 technical security controls

José Manuel Redondo López

Ubuntu 18.04 CIS Benchmark (PDF)

CSC Controls v7 (and Subcontrols)

ISO 27001:2013 Technical Security Controls

All technical security controls belonging to Subcontrol 4.9

CSC Control 4 – Controlled use of Administrative Privileges

- *4.9 Log and Alert on Unsuccessful Administrative Account Login*

All technical security controls belonging to Subcontrols 12.11 and 12.12

CSC Control 12 – Boundary Defense

- *12.11 Require all Remote Login to Use Multi-Factor Authentication*
- *12.12 Manage All Devices Remotely Logging into Internal Network*

All technical security controls belonging to Subcontrols 16.6 and 16.8

CSC Control 16 – Account Monitoring and Control

- *16.6 Maintain an Inventory of Accounts*
- *16.8 Disable Any Unassociated Accounts*

A.9: Access Control

…

A.9.4.2: Secure log-on procedures

Map to*

…

A.9.2.1: User registration and de-registration

Map to*

If instead of PDFs we had the non-free SCAP-compatible CIS Benchmark, this could have been done much easier!

*** Not every ISO 27000 control has a CSC Controls equivalent: The A5, A15, and A17 currently lacks an equivalent**

PLAN: CREATE THE FINAL SECURITY PLAN

José Manuel
Redondo López

- **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
  - Budget
  - Estimated resources (HR, materials…) and timetable to implement the actions

DO: IMPLEMENT RISK MANAGEMENT PROCEDURES

José Manuel
Redondo López

- **The next phase consist on implementing the controls and procedures**
  - The hardening automation technologies we explained may be a major help
- **They must allow quick detection and response of security incident**
- **This phase also contemplates resource, responsibility and priority assignments**

DO: USER TRAINING

José Manuel
Redondo López

- **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**

CHECK: MEASURE CONTROLS EFFECTIVENESS

José Manuel
Redondo López

- **Define a system to measure the results obtained from applying controls**
- **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**
  - **Network Access control**: Firewall stats -> attempts to access forbidden web pages
  - **Cryptography controls**: Percentage of systems that handle sensitive or valuable data and use proper cryptography methods

CHECK: MONITOR AND REVIEW

José Manuel
Redondo López

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

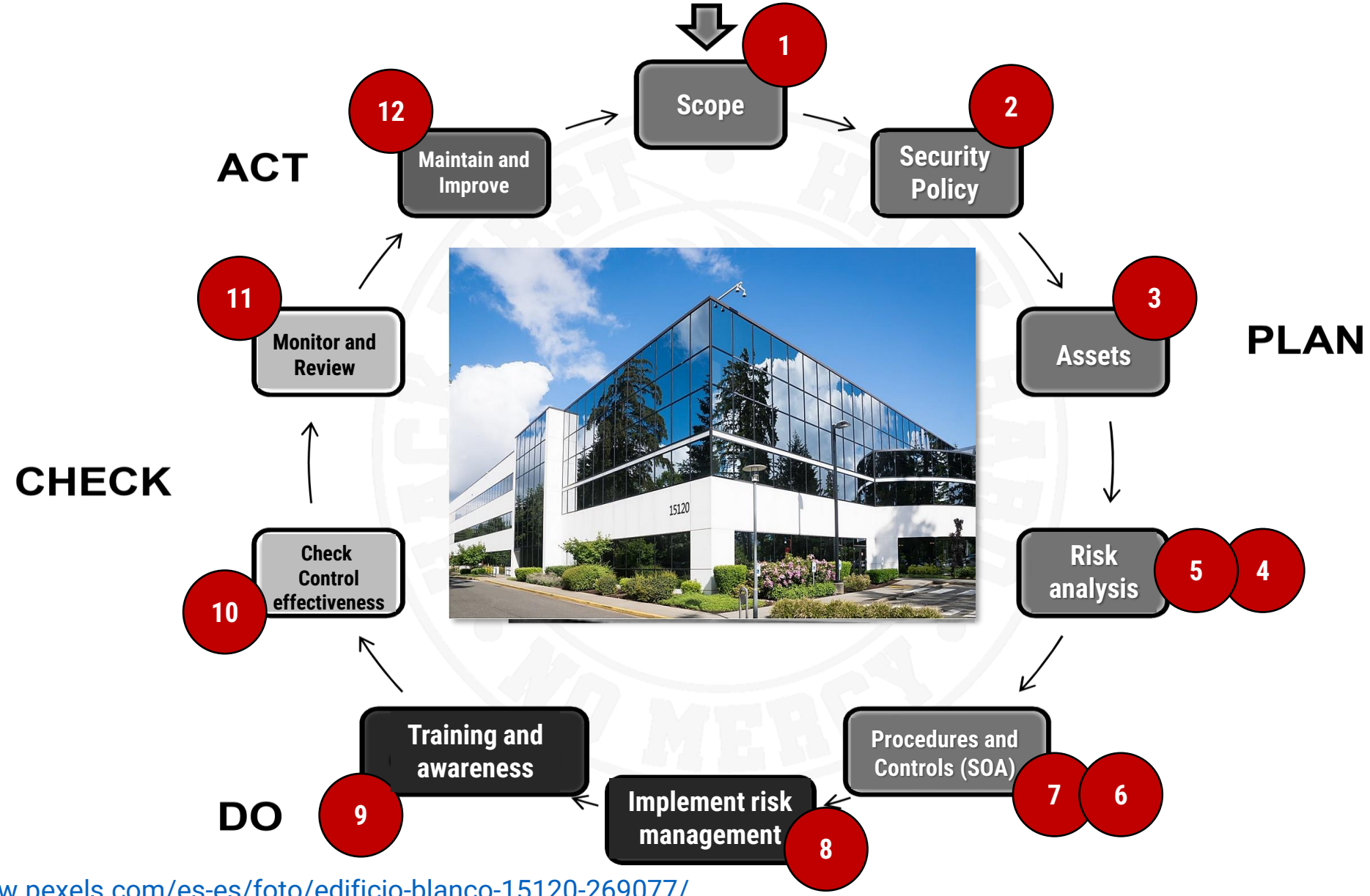
ACT: MAINTAIN AND IMPROVE THE ISMS

José Manuel
Redondo López

- **The organization shall regularly**
  - Implement the identified **improvements** in the ISMS
  - Perform appropriate preventive and corrective actions in relation to clause 8 of ISO 27001 (continuous improvement)
    - 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 targets

SUMMARY: ISMS IMPLEMENTATION

José Manuel
Redondo López



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

< Go to Index

Security audit and review methodologies: OSSTMM

How can we use this?

Source: zona-militar.com

From security controls to methodologies

José Manuel
Redondo López

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 subcontrols 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 CIS CSC Subcontrols to my particular scenario — 3

Can be distributed into

Group the implemented security controls in CIS Critical Security Controls (CSC) (20) and **subcontrols** (170 maximum, normally far less) — 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

DIAGNOSING SECURITY

José Manuel
Redondo López

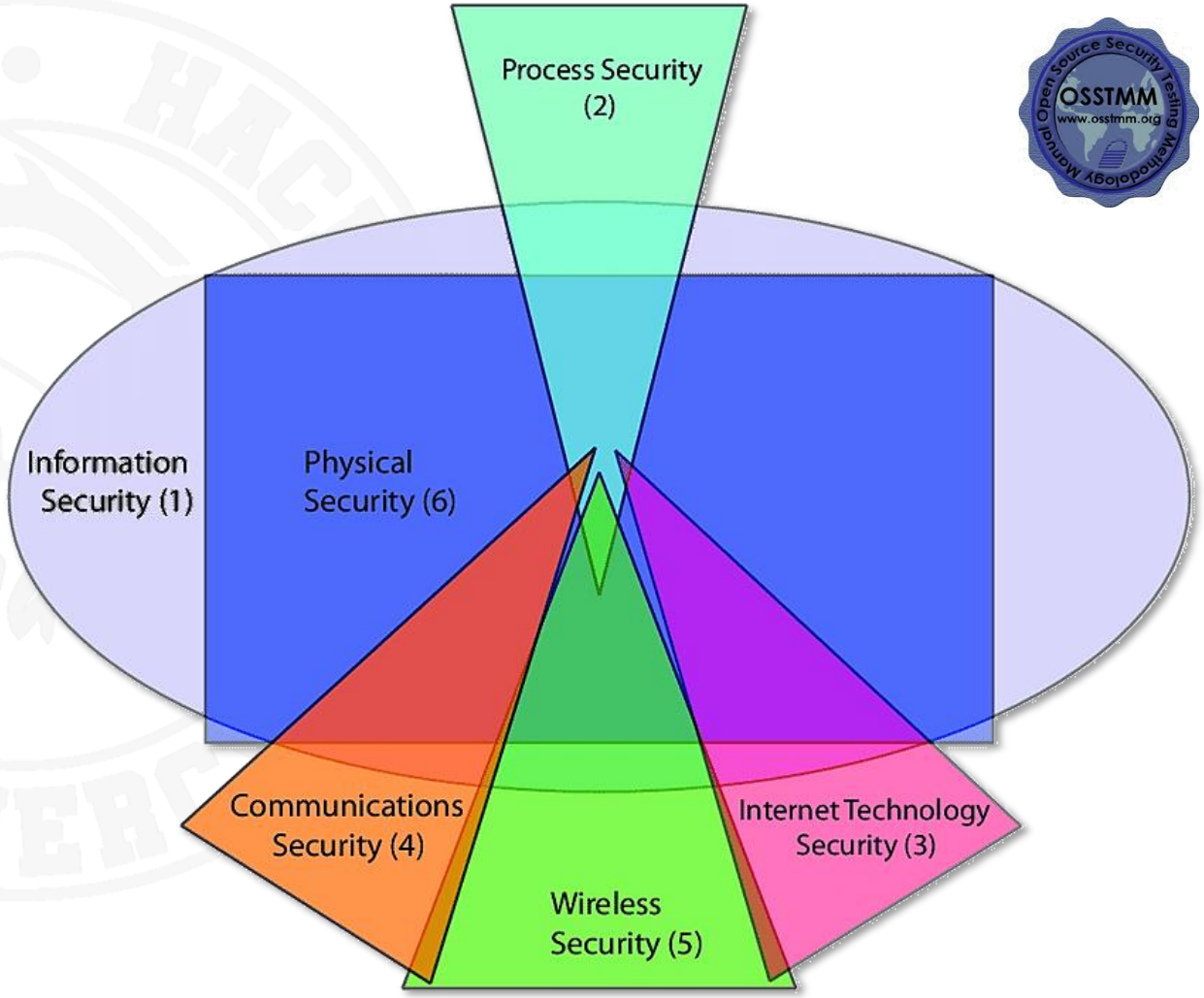
- **It is necessary to perform an exhaustive security test on each section that have security concerns to initiate any of the ISO 27001 phases**
  - This will determine the vulnerabilities of the organization's assets
- **The OSSTMM (Open-Source Security Testing Methodology Manual) security audit methodology is 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

OSSTMM SECTIONS

José Manuel
Redondo López

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

José Manuel
Redondo López

- 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

José Manuel
Redondo López

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 with users or system passwords
- List of systems vulnerable to password decryption attacks
- List of files or documents vulnerable to password decryption attacks
- List of systems with user or system accounts using the same passwords

OSSTMM: Password decryption example

José Manuel
Redondo López

- **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 their variations to access additional systems or applications
  - Start automated decryption programs in 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**

CYBERSECURITY INCIDENT RESPONSE (IR) MATURITY ASSESSMENT

José Manuel
Redondo López

- **We not only have security audit and review methodologies**
  - But also, incident response ones
- **They enable the assessment of the cyber security incident response capability status of an organization**
- **One of the most popular ones is this one, developed by CREST**
  - https://www.crest-approved.org/cyber-security-incident-response-maturity-assessment/index.html

PHASE 1
Prepare

- Step 1. Conduct a criticality assessment for your organisation
- Step 2. Carry out a cyber security threat analysis, supported by realistic scenarios and rehearsals
- Step 3. Consider the implications of people, process, technology and information
- Step 4. Create an appropriate control framework
- Step 5. Review your state of readiness in cyber security incident response

PHASE 2
Respond

- Step 1. Identify cyber security incident
- Step 2. Define objectives and investigate situation
- Step 3. Take appropriate action
- Step 4. Recover systems, data and connectivity

PHASE 3
Follow Up

- Step 1. Investigate incident more thoroughly
- Step 2. Report incident to relevant stakeholders
- Step 3. Carry out a post incident review
- Step 4. Communicate and build on lessons learned
- Step 5. Update key information, controls and processes
- Step 6. Perform trend analysis

Source: https://www.lifars.com/2021/03/crest-incident-response-maturity-assessment/

And now?

José Manuel
Redondo López

- **Implementing a full ISMS is way 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
  - This way, we have a way to quickly achieve hardening of a system in an efficient way
  - And, with time, use this to implement something more complex on a higher abstraction level
  - Best of both worlds! ☺

Self-evaluation achievement list: Automated security

José Manuel
Redondo López

Rank	Concept
	Know the SCAP hardening automation protocol and its components
	Know what the SCAP security guide package offers
	Know what the STIGs offer
	Know what the CIS benchmark offers and the difference with other security control sources
	Understand the CIS Control and subcontrols approach
	Understand the intended usage of Implementation Groups
	Know how to use security controls to facilitate security framework implementation
	Understand the procedures followed to perform security audit and review methodologies
	Understand how an ISMS is implemented
	Identify and choose the best security control list for a particular problem
	**This world doesn't need a hero, it needs a professional:** Master the previous concepts

SECURITY POLICIES AND AUTOMATED HARDENING