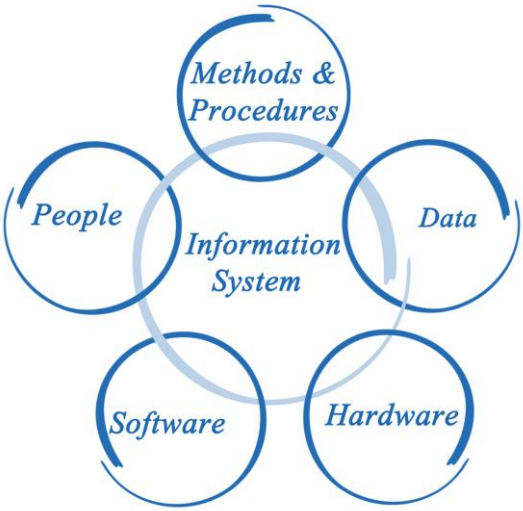
SECURING INFORMATION SYSTEMS

OVERVIEW

Prof. Dr. Bernhard Tellenbach

Information System



- Set of applications, services, information technology assets or other information-handling components [SOURCE: ISO/IEC 27000:2018, 3.35]
- Including developing and operating it, it involves
  - Methods and procedures
  - Data
  - Technology (software/hardware)
  - People

Fundamental Questions

- How do we manage information security so that an information system (or an entire organization) is secure and stays secure?

- How do we know that we are secure?

Goals

- You know what it means to secure information systems and understand that it is a many-faceted problem that no single person can learn to address/solve on its own
- You know an example of a best practice guide on important security controls to secure information systems and understand its role and level of detail
- You understand that security is difficult to measure, and you know some options on how to deal with it

BSI: *Bundesamt für Sicherheit in der Informationstechnik*

There are a lot of competing ISMS. The following three are the most popular ones:

- ISO/IEC 27000 family
  - Overview: https://en.wikipedia.org/wiki/ISO/IEC_27000-series
- NIST Risk Management Framework
  - Mainly NIST Special Publication 800-[60, 53, 30, 18, 70, 53A, 37]
  - Overview: http://csrc.nist.gov/groups/SMA/fisma/framework.html
- *BSI 200 familiy («IT-Grundschutz»*, Germany)
  - Overview: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html

Information Security Management System (ISMS)

Risk Management Framework (RMF)

- An ISMS is a systematic approach to managing information so that it remains secure.
- It includes people, processes and IT systems by applying a risk management process.
- Information security risk is managed and kept at an acceptable level by designing, implementing and maintaining a coherent set of security controls
- Our focus: Security controls

BSI: *Bundesamt für Sicherheit in der Informationstechnik*

There are a lot of competing ISMS. The following three are the most popular ones:

- ISO/IEC 27000 family
  - Overview: https://en.wikipedia.org/wiki/ISO/IEC_27000-series
- NIST Risk Management Framework
  - Mainly NIST Special Publication 800-[60, 53, 30, 18, 70, 53A, 37]
  - Overview: http://csrc.nist.gov/groups/SMA/fisma/framework.html
- *BSI 200 familiy («IT-Grundschutz»*, Germany)
  - Overview: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html

Security Controls

- Security controls are safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets.
- Controls are characterized (and sometimes grouped) by various attributes, for example type, information security property, function, and category.
  - Information security properties: Which characteristics of information does the control help to preserve *[Confidentiality, Integrity, Availability]*
  - Category: What it concerns *[people, physical objects, technology, other (organizational)]*
  - Function: The function within the ISMS *[identify, protect, detect, respond, recover]*

Function:

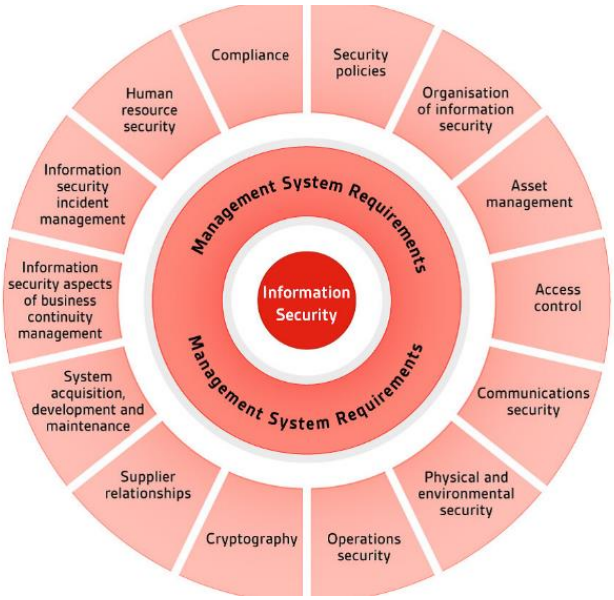
- **Identify:** The Identify Function assists in developing an organizational understanding to managing cybersecurity risk to systems, people, assets, data, and capabilities. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples:
  - Identifying physical and software assets within the organization to establish the basis of an Asset Management program
  - Identifying a Risk Management Strategy for the organization including establishing risk tolerances
- **Protect:** The Protect Function outlines appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples:
  - Protections for Identity Management and Access Control within the organization including physical and remote access
  - Empowering staff within the organization through Awareness and Training including role based and privileged user training
- **Detect:** The Detect Function defines the appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events. Examples:
  - Ensuring Anomalies and Events are detected, and their potential impact is understood
  - Implementing Security Continuous Monitoring capabilities to monitor cybersecurity events and verify the effectiveness of protective measures including network and physical activities

- **Respond:** The Respond Function includes appropriate activities to take action regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident. Examples:
    - Ensuring Response Planning process are executed during and after an incident
    - Mitigation activities are performed to prevent expansion of an event and to resolve the incident
- **Recover:** The Recover Function identifies appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident. Examples:
    - Ensuring the organization implements Recovery Planning processes and procedures to restore systems and/or assets affected by cybersecurity incidents

Attribute: Type of a Control

- Preventive controls prevent an incident from occurring, e.g., by locking out unauthorized intruders (authentication, firewall)
- Detective controls identify and characterize an incident in progress, e.g., by sounding the intruder alarm and alerting the security team (burglar alarm, intrusion detection system)
- Corrective controls limit the extent of damage caused by the incident, e.g., by recovering the organization to normal working status as efficiently as possible (backup system, redundant systems)

Controls in ISMS – Abstraction Level



- The abstraction level at which ISMS operate is usually high so that it applies to all types of organizations and sectors
- Controls might be specified/identified at different levels of granularity
- There might be specific sets of controls for certain sectors/industries
- Little guidance on how to technically implement security controls is provided

Example: ISO 27k

- ISO 27001:2022 lists 93 security controls in its Annex A
  - Network Security: "Networks and network devices should be secured, managed and controlled to protect information in systems and applications"
  - Secure disposal or re-use of equipment: "Items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use."
- ISO 27002:2022 adds implementation guidance to these controls
  - Provides a list of commonly accepted control objectives and best practice controls to be used as implementation guide when selecting and implementing controls
  - Not all control objectives and controls linked to them may be relevant to every organization
  - Extensions with industry specific guidelines exist (e.g., for telco ISO/IEC27011)
- **How specific and practical is it from a technical point of view? => Example: Controls against Malware**

ISO27002 outlines security controls and their objectives. The information security controls are generally regarded as best practice means of achieving those objectives. For each of the controls, implementation guidance is provided. Specific controls are not mandated since:

- Each organization is expected to undertake a structured information security risk assessment process to determine its specific requirements before selecting controls that are appropriate to its particular circumstances. The introduction section outlines a risk assessment process although there are more specific standards covering this area such as ISO/IEC 27005. The use of information security risk analysis to drive the selection and implementation of information security controls is an important feature of the ISO/IEC 27000-series standards: it means that the generic good practice advice in this standard gets tailored to the specific context of each user organization, rather than being applied by rote. Not all of the **39 control objectives** are necessarily relevant to every organization for instance, hence entire categories of control may not be deemed necessary. The standards are also open ended in the sense that the information security controls are 'suggested', leaving the door open for users to adopt alternative controls if they wish, just so long as the key control objectives relating to the mitigation of information security risks, are satisfied. This helps keep the standard relevant despite the evolving nature of information security threats, vulnerabilities and impacts, and trends in the use of certain information security controls.
- It is practically impossible to list all conceivable controls in a general purpose standard. Industry-specific implementation guidelines for ISO/IEC 27001:2013 and ISO/IEC 27002 offer advice tailored to organizations in the telco industry (see ISO/IEC 27011) and healthcare (see ISO 27799), with additional guidelines for the financial services and other industries in preparation.

ISO 27003:2017 provides guidance for those implementing the ISO27k standards, covering the *management system* aspects in particular. Its scope is simply to "provide explanation and guidance on ISO/IEC 27001:2013." The language of ISO/IEC 27001:2013 is inevitably rather formal, curt and stilted. ISO/IEC 27003 offers *pragmatic* explanation with *plain-speaking* advice and guidance for implementers of ISO 27001:2013.

ISO/IEC27002:2022 – Control: Protection against malware (1)

Attributes used in ISO27002:2022

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective #Corrective	#Confidentiality #Integrity #Availability	#Protect #Detect	#System_and_network_security #Information_protection	#Protection #Defence

Control

Protection against malware should be implemented and supported by appropriate user awareness.

Purpose

To ensure information and other associated assets are protected against malware.

Guidance

Protection against malware should be based on malware detection and repair software, information security awareness, appropriate system access and change management controls. Use of malware detection and repair software alone is not usually adequate. The following guidance should be considered:

a) implementing rules and controls that prevent or detect the use of unauthorized software [e.g. application allowlisting (i.e. using a list providing allowed applications)] (see 8.19 and 8.32);

b) implementing controls that prevent or detect the use of known or suspected malicious websites (e.g. blocklisting);

c) reducing vulnerabilities that can be exploited by malware [e.g. through technical vulnerability management (see 8.8 and 8.19)];

d) conducting regular automated validation of the software and data content of systems, especially for systems supporting critical business processes; investigating the presence of any unapproved files or unauthorized amendments;

e) establishing protective measures against risks associated with obtaining files and software either from or via external networks or on any other medium;

What attribute values apply?

ISO/IEC27002:2022 – Control: Protection against malware (2)

f) installing and regularly updating malware detection and repair software to scan computers and electronic storage media. Carrying out regular scans that include:

   1) scanning any data received over networks or via any form of electronic storage media, for malware before use;

   2) scanning email and instant messaging attachments and downloads for malware before use. Carrying out this scan at different places (e.g. at email servers, desktop computers) and when entering the network of the organization;

   3) scanning webpages for malware when accessed;

g) determining the placement and configuration of malware detection and repair tools based on risk assessment outcomes and considering:

   1) defence in depth principles where they would be most effective. For example, this can lead to malware detection in a network gateway (in various application protocols such as email, file transfer and web) as well as user endpoint devices and servers;

   2) the evasive techniques of attackers (e.g. the use of encrypted files) to deliver malware or the use of encryption protocols to transmit malware;

h) taking care to protect against the introduction of malware during maintenance and emergency procedures, which can bypass normal controls against malware;

⋮

Other information

It is not always possible to install software that protects against malware on some systems (e.g. some industrial control systems). Some forms of malware infect computer operating systems and computer firmware such that common malware controls cannot clean the system and a full reimaging of the operating system software and sometimes the computer firmware is necessary to return to a secure state.

Implementing an ISMS

- Implementation of an ISMS is a task for the management
  - Typically, its the Chief Information Security Officer's (CISO) task
  - CISO: Motivates investments, talks to the board in business- and risk-terms
- ISMS is the key to get the big picture of what it means to manage the security of an information system as a whole
- Standards can be viewed as a sort of "checklist" to not to forget relevant aspects of managing risk and security
  - Certification: Checks whether the company implements a standard
- Implementing an ISMS is complex and takes a lot of effort and time
- No guidance to efficiently direct resources to combat the most common threats that result in the greatest number of attack vectors

=> CIS Critical Security Controls

The **Center for Internet Security** (CIS) is a 501(c)(3) not-for-profit organization founded in October, 2000, whose mission is to "enhance the cyber security readiness and response of public and private sector entities, with a commitment to excellence through collaboration." It is composed of roughly 180 members from 17 different countries. CIS strives to improve global internet security by creating and fostering a trustable and secure environment to bridge the public and private sectors. In addition, at the national and international level, CIS plays an important role in forming security policies and decisions. CIS has four divisions: the Central Intelligence Center, the Multi-State Information Sharing and Analysis Center (MS-ISAC), Security Benchmarks, and the Trusted Purchasing Alliance. Through these four divisions, the Center for Internet Security works with a wide range of entities, including those in academia, the government, and both the private sector and general public to increase their online security by providing them with products and services that improve security efficiency and effectiveness.

Check out https://msisac.cisecurity.org/ for more information.

CIS Controls

- Best-practice guidelines whose development started in 2008, triggered by massive data breaches at organizations in the US defense industry.
- Consist of 18 controls for dealing with current cyber attacks
- Created and revised by experts from many different organizations
- Guiding principles:
  - Include only critical security controls
    - Based on knowledge of attacker behavior and how to defend against it
    - Whenever possible, base the selection of a control for the CIS controls on data.
  - Prioritize a control as a community, while emphasizing that own, better-informed risk assessments are desirable
  - Immediate action is more important than elegance and completeness of action
  - Provide information on how to implement and automate controls

The **best practice guidelines** "CIS Controls" is also known as:
- The CIS Critical Security Controls (from 2015 v6.0 to 7.1)
- The SANS Top 20 Critical Security Controls (before 2013, where ownership was with SANS)
- The Consensus Audit Guidelines (CAG) (rarely used, old)

Development: In 2008, the National Security Agency started an effort to efficiently direct resources to combating the most common network vulnerabilities that resulted in the greatest number of attack vectors. While the initiative initially remained classified, access to the control-prioritization strategy was eventually extended to other government entities, the administrators of critical infrastructure, and then opened up to wide variety of stakeholders charged with protecting sensitive data and systems. The best practice guidelines now represent the mind-share from a broad coalition of experts representing government, private industry, researchers and academia.

Guiding principles: All general principles for the CIS Controls and goals for v8 can be found here:
- https://workbench.cisecurity.org/files/3125/download/3866

CIS Controls (Critical Security Controls)

#safeguards in Implementationgroup IG1, IG2, und IG3

Safeguards: Things that should get implemented (sub-controls prior to v8)

CIS Control: Content

- Overview
  - A brief description of the purpose of the control and its usefulness as a defensive measure.
- Why is this control important?
  - A description of the importance of this control in blocking, mitigating or detecting attacks and an explanation of how attackers exploit the absence of this control.
- Processes and tools
  - A more technical description of the processes and technologies that enable the implementation and automation of this control.
- Safeguards
  - A table of specific measures that should be taken to implement the control.

CIS Controls – Prioritization (1)

- Until v7.1:
  - At the control level: Low numbers (1-6) were understood as so-called "cyber hygiene" and should be implemented before the other controls.
  - This view was criticized as being too simplistic – the remaining controls were delayed/not implemented because the implementation of the some of the controls 1-6 was too complex.
- Since v8:
  - Prioritization at the level of measures (safeguards) is now carried out by means of the implementation groups IG1 to IG3.
  - The order of the controls still has a certain value
    - For example, controls 1 and 2 are more effective in protecting against malware than control 10.
- In practice:
  - Can serve as a guideline/baseline
  - A cost-benefit analysis should be carried out for each environment (=> RISK ASSESSMENT)
    - Available resources and expected implementation time should be considered.

Prioritization

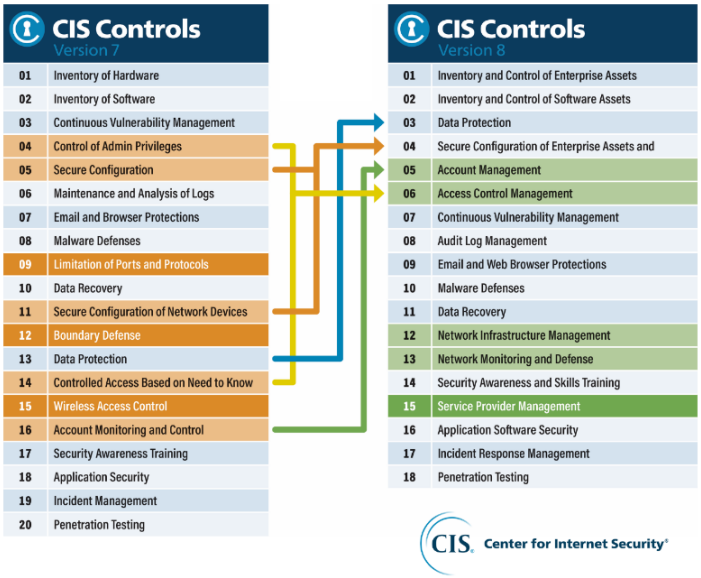
CIS Controls v7.1

CIS Controls 1 through 6 are essential to success and should be considered among the very first things to be done. We refer to these as “Cyber Hygiene” – the basic things that you must do to create a strong foundation for your defense. This is the approach taken by, for example, the DHS Continuous Diagnostic and Mitigation (CDM) Program, one of the partners in the CIS Controls.
A similar approach is recommended by our partners in the Australian Signals Directorate (ASD) with their “Essential Eight” – a well-regarded and demonstrably effective set of cyber defense actions that map very closely into the CIS Controls. This also closely corresponds to the message of the US-CERT (Computer Emergency Readiness Team).
Source: CIS Controls, 7.1, Center for Internet Security

CIS Controls v8

Historically, the CIS Controls were ordered in sequence to focus an enterprise’s cybersecurity activities, with a subset of the first six CIS Controls referred to as “cyber hygiene.” However, this proved to be too simplistic. Enterprises, especially small ones, could struggle with some of the early Safeguards and never get around to implementing later CIS Controls (for example, having a backup strategy to help recover from ransomware). As a result, starting with Version 7.1, we created CIS Controls Implementation Groups (IGs) as our recommended new guidance to prioritize implementation.

CIS Controls – Prioritization (2)



See https://www.sans.org/blog/cis-controls-v8/ and the material available at the CIS WorkBench for more detailed information on the changes and their motivation.

CIS Controls – Implementation Group IG1

- IG1 - Basic Cyber Hygiene
  - Safeguards that can be implemented even with limited cyber security expertise.
  - Designed to thwart general, non-targeted attacks
  - Designed for use with COTS hardware and software in small businesses or home offices.
  - Used to protect IT resources and personnel.
- Is IG1 secure enough? No, but you could stop here if …
  - you are an SME with limited IT and cybersecurity skills.
  - your primary interest is in maintaining business operations
  - the sensitivity of the data to be protected is low and mainly concerns employee and financial information

COTS = commercial off-the-shelf

CIS Controls – Implementation Group IG2

- IG2 (IG1 included)
  - Helps security teams cope with increasing operational complexity
  - Often requires enterprise-grade technology and requires specific cybersecurity expertise
- Reasons to implement IG2
  - Multiple departments with different risk profiles based on responsibilities and mission.
  - Business units must adhere to compliance regulations.
  - Retention and processing of sensitive customer or company data
  - A major concern is the loss of public trust if a breach occurs.

CIS Controls – Implementation Group IG3

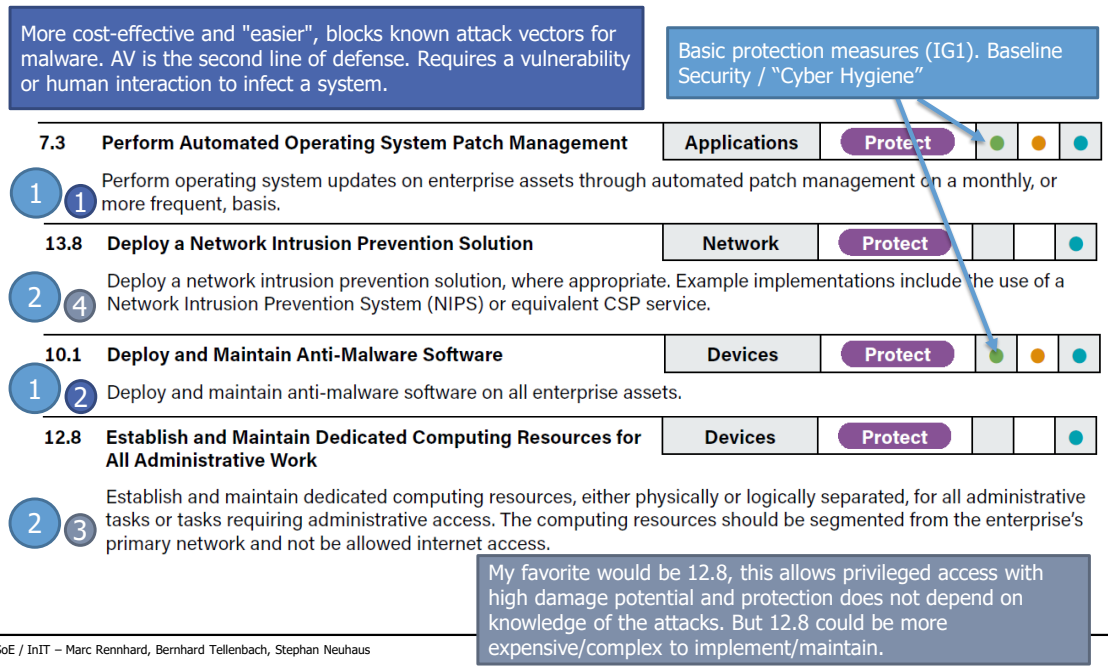
- IG3 (includes IG1 and IG2)
  - Requires security experts from different security areas
    - e.g., risk management, penetration testing, application security.
  - Protective measures help against targeted attacks by sophisticated adversaries
  - Protective measures help reduce the impact of zero-day attacks
- Reasons to implement IG3:
  - Retention and handling of sensitive information/functions subject to regulatory oversight and compliance.
  - The availability of services and the confidentiality and integrity of sensitive data are at the heart of the business.
  - Attacks can cause significant harm to the public.

CIS Controls – Exercise «Priority»

- Below is a selection of protective measures from various controls - in what order would you implement them and why?

7.3	**Perform Automated Operating System Patch Management** Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	**Applications**	
13.8	**Deploy a Network Intrusion Prevention Solution** Deploy a network intrusion prevention solution, where appropriate. Example implementations include the use of a Network Intrusion Prevention System (NIPS) or equivalent CSP service.	**Network**	
10.1	**Deploy and Maintain Anti-Malware Software** Deploy and maintain anti-malware software on all enterprise assets.	**Devices**	
12.8	**Establish and Maintain Dedicated Computing Resources for All Administrative Work** Establish and maintain dedicated computing resources, either physically or logically separated, for all administrative tasks or tasks requiring administrative access. The computing resources should be segmented from the enterprise's primary network and not be allowed internet access.	**Devices**	

CIS Controls – Exercise «Priority»



Note: While the IGs are indicative for the prioritization, the numbering of the controls is not. Nevertheless, for safeguards with the same IGs, you might use it as a starting point to think about them.

- Does the control help mitigate one of your main concerns/risks? For example, is it likely, that skilled hackers invest lots of resources to attack you?
- Do they depend on knowledge about attacks or are they independent of such knowledge? (negative)
- Does the safeguard need a lot of manual labor to setup and even more important, to manage/maintain? (negative)
- Does the control impact employee's workflows in a negative way?
- How many assets/processes need to be modified/changed? (many: negative)
- Considering you assets/risk profile/infrastructure – is the control relevant at all?
- …

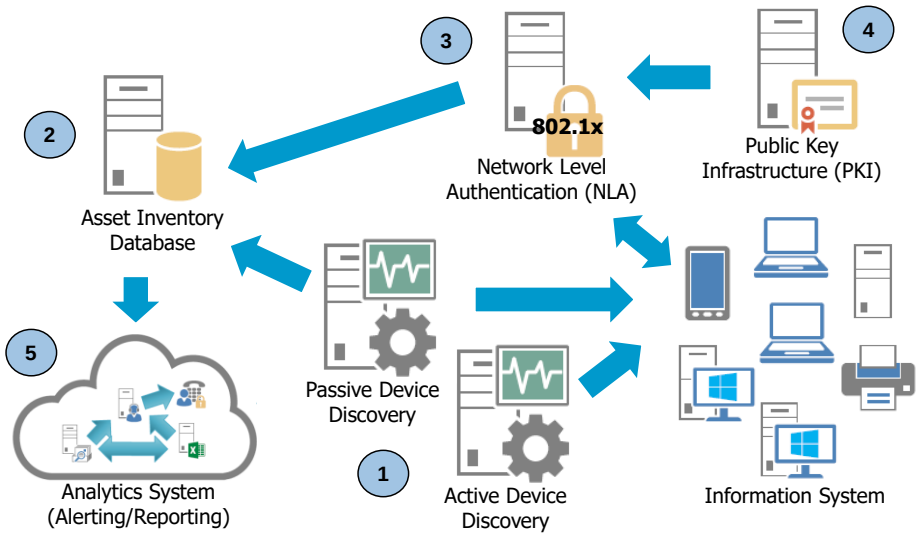
However, in general, as noted earlier, such decisions should be based on a systematic risk assessment.

CIS Controls – A more detailed look

- What we will do now:
  - Discuss controls 1, 2 (and eventually 7)
  - Discover why Control 2 is very effective against malware.
- Other controls:
  - Have a look at them yourself

- Key take aways:
  - Get an idea of the complexity and the numerous components and activities involved when implementing a control. Granularity: (technical) measures and building blocks.
  - Gain insight into a (prominent) example of a guideline for the implementation of security controls.

CSC 1: Inventory and Control of Enterprise Assets



Goal:

- Actively manage all hardware devices on the network so that **only authorized devices are given access**, and unauthorized and **unmanaged devices** are found and **prevented from gaining access**.

Rationale:

Attackers continuously **scan** address spaces for new systems that might (yet) be unprotected
People with physical access to the network might **attach unauthorized devices** (demonstrators, test systems, access points, Playstation,…)

Implementation:

1. Use **active (scanning, e.g. nmap)** and passive **(arp/dhcp monitoring [e.g., arpwatch], traffic monitoring [e.g., PADS])** device detection tools to build an asset inventory.
2. The inventory should store at least: network addresses, machine name(s), purpose, asset owner, department
3. Deploy **network level authentication via 802.1x** to limit and control which devices can be connected to the network.
   The 802.1x must be tied into the inventory data to determine authorized versus unauthorized systems.
4. Use *client certificates* to validate and authenticate systems prior to connecting to private network.
5. Attach the Asset Inventory to an analytics system **for alerting** and to make use of the inventory **to correlate assset data** with other data.
   For example, if the intrusion detection system reports that host X has been infected by

WIN32.RANSOM but the host is running Linux, this might be flagged as a false positive.

Products/Software* Examples:
Usually, this is one of the components of a SIEM system. We'll have a closer look at SIEMs later.
Some examples of commercial SIEM including this capability:

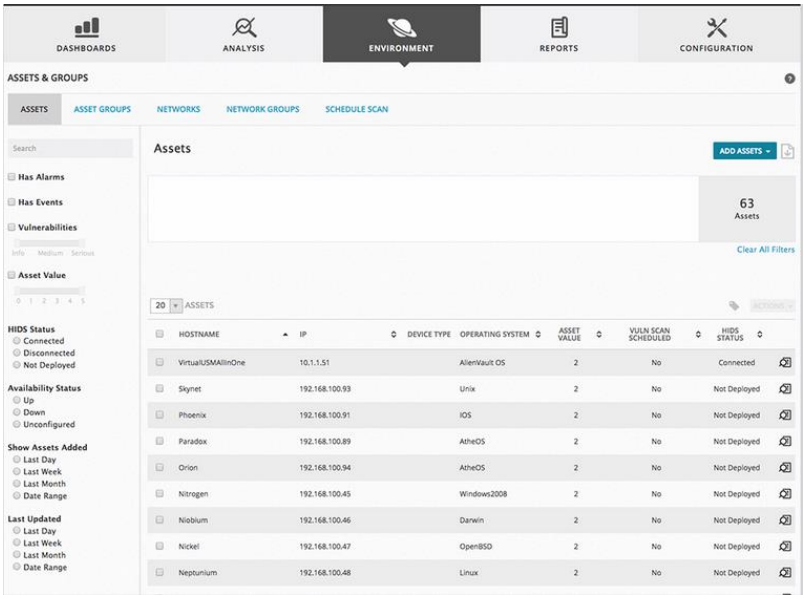
- SecurityCenter (Tenable)
- AlienVault Unified Security Management™ (USM)
- LogRythm SIEM

Free and Open Source SIEM:

- AlienVault OSSIM

*Note that the products/software landscape is changing quickly and some or all of the products listed here might not exist anymore

CSC 1: Inventory and Control of Enterprise Assets



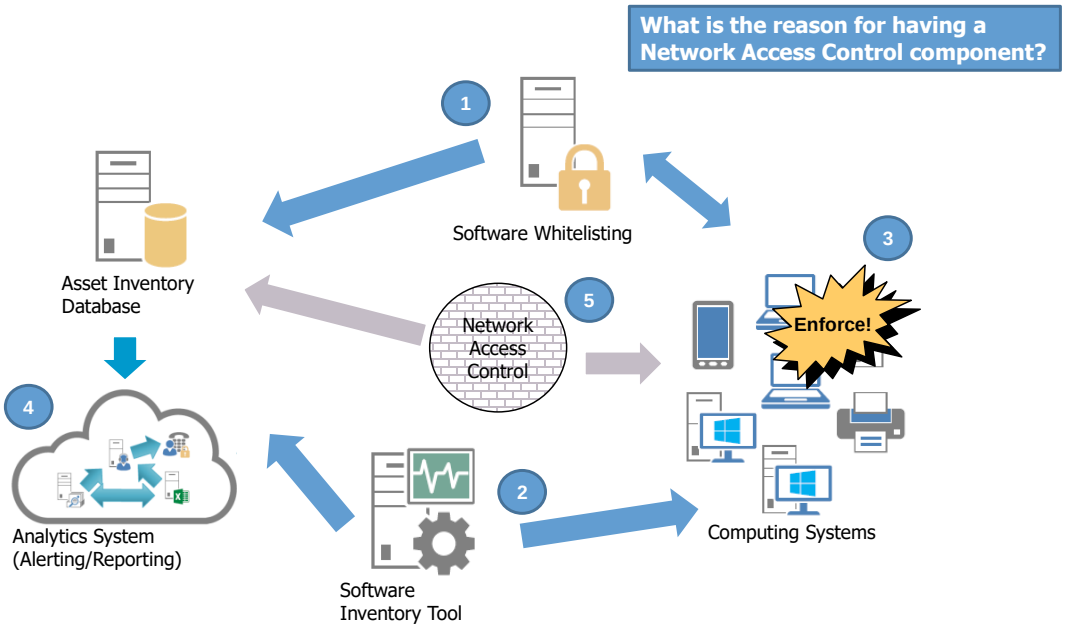
Exercise

- Question: Why is it useful to use both active and passive device search tools?

CSC 1: Sub-Control Level

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
1.1	**Establish and Maintain Detailed Enterprise Asset Inventory** Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, data asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.	Devices	Identify	●	●	●
1.2	**Address Unauthorized Assets** Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.	Devices	Respond	●	●	●
1.3	**Utilize an Active Discovery Tool** Utilize an active discovery tool to identify assets connected to the enterprise's network. Configure the active discovery tool to execute daily, or more frequently.	Devices	Detect		●	●
1.4	**Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory** Use DHCP logging on all DHCP servers or Internet Protocol (IP) address management tools to update the enterprise's asset inventory. Review and use logs to update the enterprise's asset inventory weekly, or more frequently.	Devices	Identify		●	●
1.5	**Use a Passive Asset Discovery Tool** Use a passive discovery tool to identify assets connected to the enterprise's network. Review and use scans to update the enterprise's asset inventory at least weekly, or more frequently.	Devices	Detect			●

CIS 2: Inventory and Control of Software Assets



Goal:

- Actively manage all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation/execution.

Rationale:

- Attackers continuously try to find vulnerable versions of software by **scanning** the address spaces or by making use of information from an organization's websites, publications or employees
- Employees install/run software from third parties that might cause problems because it contains malware or because it is not inline with the policy of the company.

Implementation:

1. Devise a white-list of authorized software and version that is required in the enterprise
2. Deploy a software inventory tool to track the operating system and applications installed on each asset
3. Deploy application whitelisting that allows systems to run software only if it is included on the whitelist.
4. Attach the Asset Inventory to an analytics system **for alerting** and to make use of the inventory **to correlate assset data** with other data.
   For example, if the intrusion detection system reports an attack on vulnerability CVE-2015-7547 but the system runs a non-vulnerable version of glibc, this might be flagged as a false positive.

5. Network access control
    1. Segregate high risk applications for business operation
    2. Block systems from accessing the network that do not comply to the rules regarding the installed software

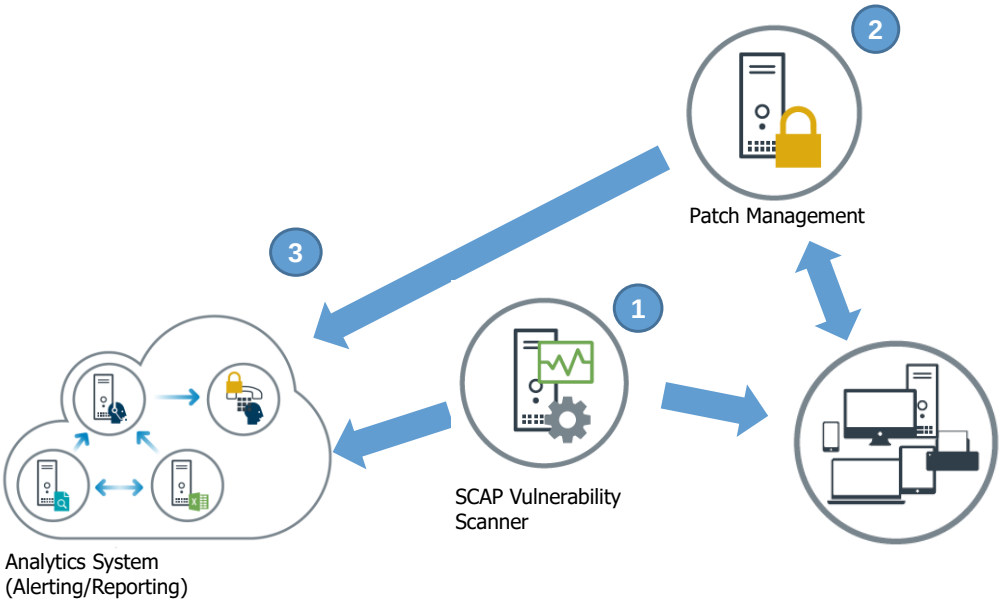
Products/Software* Examples:
This CSC is addressed by two types of products:
Software Change Management products (maybe also Vulnerability Management)
- SecurityCenter (Tenable)
- System Center (Microsoft)

Application Whitelisting products
- Security Platform (Bit9)

An example of a free and open source product is:
- OCS Inventory NG (HW & SW inventory system, no application whitelisting)

*Note that the products/software landscape is changing quickly and some or all of the products listed here might not exist anymore

CIS 7: Continuous Vulnerability Management



Goal:

- Continuously **acquire, assess, and take action** on new information in order **to identify vulnerabilities**, **remediate**, and **minimize the window of opportunity** for attackers.

Rationale:

- New vulnerabilities are discovered every day
- Attackers can **take advantage of gaps** between the **appearance** of new knowledge and **remediation**.
- Defenders face particular challenges in **scaling remediation** across an entire enterprise, and prioritizing actions with **conflicting priorities**, and sometimes--uncertain side effects. **Example: Heartbleed** – Took up to several days to roll-out the updates. Even weeks or longer for products that came with their own version of OpenSSL compiled in.

Implementation:

1. Deploy a **vulnerability scanning tool** and run it on **a weekly** or more frequent basis, inform the owners and inform and track their effectiveness in reducing risk. It should scan for **code-based** (e.g., CVEs) and **configuration-based** vulnerabilities (e.g., CCEs)
2. Deploy **automated patch management** and software update tools whenever such tools are available and safe.
   Patches should be applied to all systems, even systems that are properly air gapped.
3. Link it to an alerting and reporting system to track problems and progress. An analytics system (SIEM) might **correlate attack detection events** with vulnerability scanning results to determine whether a given exploit was used against a target known to be vulnerable.

Products/Software* Examples:

- Nessus (Tenable)
- QualysGuard (Qualys)

*Note that the products/software landscape is changing quickly and some or all of the products listed here might not exist anymore

CIS Controls: Adoption / Implementation

Discuss:
- Which CIS controls suggest a high acceptance rate? What could be the reason?

CSC	Partial	Full	None
1: Inventory of Authorized and Unauthorized Devices	60%	27%	12%
2: Inventory of Authorized and Unauthorized Software	64%	22%	13%
3: Secure Configurations for Hardware & Software on Mobile Devices, Laptops, Workstations, and Servers	62%	27%	10%
4: Continuous Vulnerability Assessment and Remediation	58%	28%	14%
5: Malware Defenses	47%	50%	4%
6: Application Software Security	55%	18%	26%
7: Wireless Access Control	45%	43%	12%
8: Data Recovery Capability	52%	39%	7%
9: Security Skills Assessment and Appropriate Training to Fill Gaps	54%	18%	26%
10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	51%	41%	8%
11: Limitation and Control of Network Ports, Protocols, and Services	53%	36%	9%
12: Controlled Use of Administrative Privileges	57%	34%	8%
13: Boundary Defense	45%	49%	4%
14: Maintenance, Monitoring, and Analysis of Audit Logs	63%	19%	16%
15: Controlled Access Based on the Need to Know	57%	29%	13%
16: Account Monitoring and Control	58%	26%	15%
17: Data Protection	58%	24%	16%
18: Incident Response and Management	62%	23%	15%
19: Secure Network Engineering	59%	25%	15%
20: Penetration Tests and Red Team Exercises	43%	21%	35%

Quelle: A SANS Analyst Survey, James Tarala, Tony Sager, September 2014

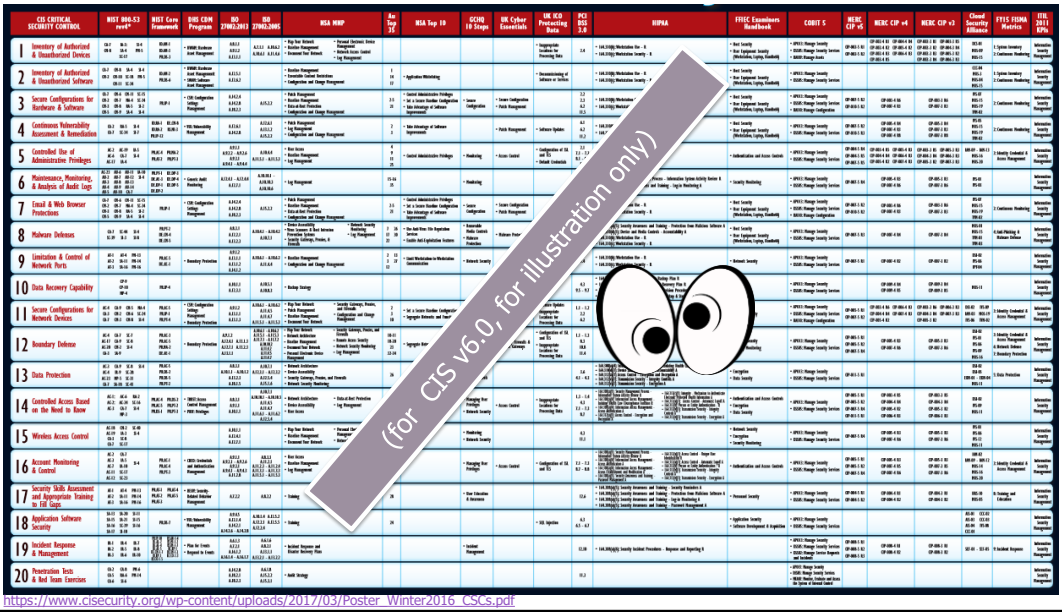
Based on CIS-CSC-version from 2014

Source: A SANS Analyst Survey, James Tarala, Tony Sager, September 2014

328 people from a **variety of businesses and government entities** completed the survey. The largest group represented was the **financial services industry** (22%), with the government sector contributing an additional 18%. Other industry verticals were also well represented, with high-tech (8%), energy/utilities (7%), education (7%), health care/pharmaceuticals (6%), telecommunications carriers and service providers (6%), and manufacturing (6%) also making strong showings.

Note: Figures do not add up to 100% due to rounding error.

Mapping of CIS Critical Security Controls to other Standards



https://www.cisecurity.org/wp-content/uploads/2017/03/Poster_Winter2016_CSCs.pdf

Relationship to other standards: The CIS Controls address mainly technical control areas. However, since most ISMS list a series of controls, the CIS Controls can be mapped to a subset of the controls listed there.
Some mappings can be found here:
- https://www.cisecurity.org/critical-controls/tools/

Example for the NIST CSF (cyber security framework):
- https://workbench.cisecurity.org/files/3328/download/4259

Summary and Criticism

- Most companies implement only a subset of the controls
- Protecting information systems is complex:
  - Guidance with checklists and implementation notes needed
  - Many resources required to implement and maintain all controls
  - Risk management required to manage what is implemented and when

- Critique
  - Paper "A Critical View on CIS Controls" by Stjepan Gros, University of Zagreb
  - Some of the criticisms are justified, some also apply to other "ISMS", and some are unjustified or very academic => see for yourself!

CISC Criticism
Overall, there are few sources that critically review or analyze the development and sales arguments of CIS. A critical view from an academic perspective is provided by the paper published on arxive.org in May 2020:
“A Critical View on CIS Controls, Stjepan Groš, Laboratory for Information Security and Privacy”, University of Zagreb
https://arxiv.org/pdf/1910.01721.pdf
Some of the questions and criticisms raised in it seem justified, but the publication does also have some weaknesses itself. It is worth reading and reflecting on the CIS (and other ISMS) yourself.

Two food for thought on this.

Criticism: "Prioritization/grouping does not help, as own risk assessment is still necessary".

CIS makes a "universal" risk assessment by prioritizing controls (number and implementation groups). This is done regarding "what is most useful against current threats". However, because the CIS Controls document then still mentions the necessity of adapting the selected controls (and their prioritization) to one's own situation using, for example, the CIS Risk Assessment Model introduced in 2018, the paper does not see the benefit - a separate risk management process would still be necessary. The following considerations could be made here: Small companies without complex IT and without much security expertise will get help here to improve their situation. It is unrealistic to assume that they can afford academic "perfection" - the CIS controls explain each control in an understandable way and explain why

it is considered important/critical.
The benefit of prioritization/grouping is not the avoidance of separate risk assessment and management. Prioritization and grouping provide a basis for discussion and in particular consider events/events from the "current" threat landscape (see also the changes via the versions of the CIS Controls).

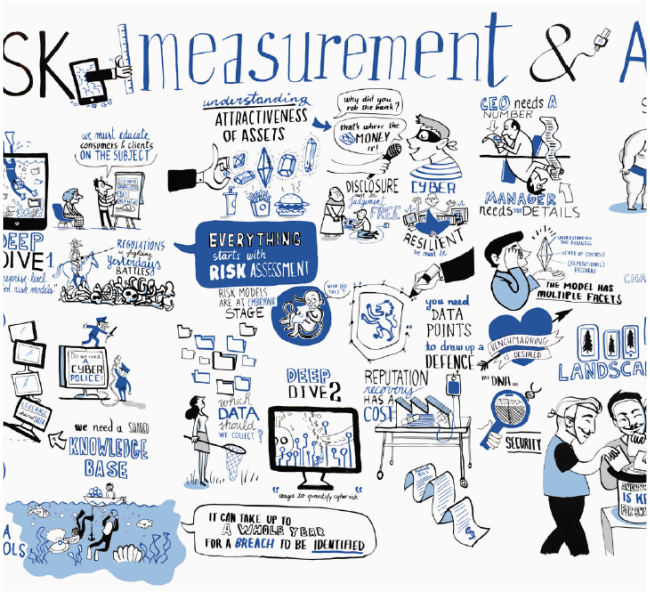
Criticism: "Methodology of how the CIS controls are developed (e.g., why prioritized in the same way?) unclear".

The author criticizes that little is known about the development process. It is true that the CIS Controls document says little more than things like "the controls were developed by a large group of well-known companies and experts" and that there was a public consultation. He claims that there is no publicly available information on this. However, this is not entirely correct. Access to the written proposals and discussions submitted during the development phase is free and open to all. One only must register with the CIS portal and can then view them and make one's own contributions. What is true is that even then it is not clear how it is finally decided which proposals/changes will be implemented.

Measuring the Security of Information Systems

Discussion

- How would you measure the security of an information system?



How Secure is your Organization?

- A (very much) incomplete list of factors influencing the security of an information system
  - People (employees and other people with access to the system)
  - Physical security (access control, alarm systems, tamper resistance,…)
  - Known and unknown (!) vulnerabilities in software and hardware
  - Controls to mitigate vulnerabilities in software and hardware
  - Configuration and architecture of hard- and software
  - Processes and policies
  - …
- Measuring the security of an information system in a scientific and holistic way is (most likely) not possible
- The same applies to measuring risk, which impacts on your process of selecting and implementing controls.

  => But what can we do then?

Approaches to Measure Security

- Security:
  - Audit - A systematic evaluation measuring how well (parts) of an information system conforms to a set of established criteria
  - Perform a penetration test
  - Using measures for the performance and effectiveness of an ISMS
- Risk:
  - Estimate the risk using something like:
    Risk = Likelihood x Impact
  - Estimation of likelihood is very difficult
  - Challenge:
    - Estimate by what activity you are more likely to catch a serious illness and by how much (see activities on the right)

Check out https://www.self.com/story/psoriasis-seborrheic-dermatitis if you want to know some more details about the tootbrush challenge.

Why should we Measure at all?

- Identify information security processes/controls that are implemented incorrectly, ineffective, not implemented at all
- Quantify improvements/progress in securing an information system
  - e.g., track the time fix a (critical) vulnerability after its discovery
  - e.g., track how resilient the employees are against phishing attacks
- Evidence required by or to help demonstrate fulfilling of standards, law and regulations (compliance)
  - e.g., to comply with ISO 27001, the performance and effectiveness of the ISMS must be evaluated
- Support risk-informed decision making
  - e.g., successes / failures of information security investments

Exercise: Measures of Performance and Effectiveness

- Have a close look at two examples of measures from:
  - NIST SP 800-55
  - ISO 27004

- Try to answer the following questions:
  - What do they measure?
  - How is this related to «security» - at what «value» is it secure enough?

Example: NIST 800-55

Measure 2: Vulnerability Management (program-level)

Goal	Ensure an environment of comprehensive security and accountability for personnel, facilities, and products Information Security Goal: Ensure all vulnerabilities are identified and mitigated.
Measure	Percentage (%) of high vulnerabilities mitigated within organizationally defined time periods after discovery. NIST SP 800-53 Controls: RA-5; Vulnerability Scanning
Measure Type	Effectiveness/Efficiency
Formula	$\frac{\#\ \textbf{of high vuln.mitigated within targeted time frame}}{\#\ \textbf{of high vulns.}}$ (in time period of length T)
Target	This should be a high percentage defined by the organization.
Implementation Evidence	# of high vulnerabilities identified across the enterprise during the time period? # of high vulnerabilities mitigated across the enterprise during the time period?
Frequency	Collection Frequency: Organization-defined (example: quarterly) Reporting Frequency: Organization-defined (example: quarterly)
Responsible Parties	Information Owner: CIO, SAISO (e.g., CISO), System Owner Information Collector: System Administrator or ISSO Information Customer: CIO, SAISO (e.g., CISO)
Data Source	Vulnerability scanning software, audit logs, vulnerability management systems, patch management systems, change management records
Reporting Format	Stacked bar chart illustrating the percentage of high vulnerabilities closed within targeted time frames after discovery over several reporting periods

CIO: Chief Information Officer
SAISO: Senior Agency Information Security Officer (e.g., CISO)
CISO: Chief Information Security Officer
ISSO: Information System Security Officer

What is NIST SP 800-55?

Abstract: This document provides guidance on how an organization, through the use of metrics, identifies the adequacy of in-place security controls, policies, and procedures. It provides an approach to help management decide where to invest in additional security protection resources or identify and evaluate nonproductive controls. It explains the metric development and implementation process and how it can also be used to adequately justify security control investments. The results of an effective metric program can provide useful data for directing the allocation of information security resources and should simplify the preparation of performance-related reports.

Source: Elizabeth Chew, Marianne Swanson, Kevin M. Stine, Nadya Bartol, Anthony Brown, and Will Robinson. 2008. SP 800-55 Rev. 1. Performance Measurement Guide for Information Security. Technical Report. National Institute of Standards & Technology, Gaithersburg, MD, USA.

Example: ISO 27004:2016

B.23 Protection against malicious code

Information descriptor	Meaning or purpose
Measure ID	Organization-defined
Information need	To assess the effectiveness of the protection system against malicious software attacks
Measure	Trend of detected attacks that were not blocked over multiple rep. periods
Formula/scoring	Number of security incidents caused by malicious software/number of detected and blocked attacks caused by malicious software
Target	Trend line should remain under specified reference, resulting in a downward or constant trend
Implementation evidence	1 Count number of security incidents caused by malicious software in the incident reports 2 Count number of records of blocked attacks
Frequency	Collect: Daily | Analysis: Monthly | Report: Monthly Measurement Revision: Review annually Period of Measurement: Applicable 1 year
Responsible parties	Information owner, Information collector, Measurement client
Data source	1 Incident reports 2 Logs of countermeasure software for malicious software
Reporting format	Trend line that depicts ratio of malicious software detection and prevention with lines produced during previous reporting periods

What is ISO 27004:2016?

The ISO 27004 document contains guidelines intended to assist organizations in evaluating the information security performance and the effectiveness of an information security management system in order to fulfil the requirements of ISO/IEC 27001. It establishes

1) the monitoring and measurement of information security performance
2) the monitoring and measurement of the effectiveness of an information security management system (ISMS) including its processes and controls
3) the analysis and evaluation of the results of monitoring and measurement

Recommendations

- Measuring the safety of an infrastructure as a whole is hardly possible
- Nevertheless, we need to measure in order to make decisions, even if the relationship to the safety of an infrastructure is not clear or not given at all.
- Measurement with the aim of reducing uncertainty about the security
- Recommendations:
  - Question what is measured, how and what data is used and what conclusions are drawn
    - "We have seen 100k failed ssh login attempts, that's twice as much as last month => significant increase in our exposure!" => Right?
  - Use comparative measurements
    - "A subnet with an intrusion detection system is more secure than one without "
    - "Applying static analysis to code makes it more secure"
  - Measure progress and maturity using best practice measures.

Summary

- Securing information systems is hard
- There are three types of controls: preventive, detective, and corrective controls
- An information security management system (ISMS) standards can offer guidance but not at a very detailed level or at a technical level
- They are handy checklists to see what controls exist and what has been implemented
- The CIS Critical Security Controls is a list of security controls with some guidance on what controls they consider most basic/relevant
- Measuring security is hard - use comparative measurements