**Vulnerability & Exploits:**

* **Vulnerability:**

In cybersecurity, a vulnerability is a weakness that can be exploited by cybercriminals to gain unauthorized access to a computer system. After exploiting a vulnerability, a cyberattack can run malicious code, install malware and even steal sensitive data.

* **Exploit:**

An exploit is a code that takes advantage of a software vulnerability or security flaw. When used, exploits allow an intruder to remotely access a network and gain elevated privileges, or move deeper into the network.

* **Vulnerability vs Exploit:**

In a nutshell, a vulnerability is a weakness or opening for hackers to find a way into a website, a system that connects to a website, operating systems, [web applications](https://sectigostore.com/blog/what-is-owasp-what-are-the-owasp-top-10-vulnerabilities/), software, networks, and other IT systems. An exploit is a specific code or attack technique that uses a vulnerability to carry out an attack or gain unauthorized access. The vulnerability is the opening and the exploit is something that uses that opening to execute an attack.

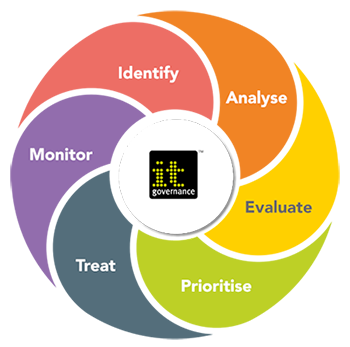
* **Risk:**

Risk is defined as the probability of an event and its consequences.

* **Risk Management:**

Risk management is the practice of using processes, methods and tools for managing these risks. Businesses that have identified the risks will be better prepared and have a more cost-effective way of dealing with them.

**Cyber risk management** is the process of identifying, analyzing, evaluating and addressing your organization’s cyber security threats. The first part of any cyber risk management program is a cyber-risk assessment.



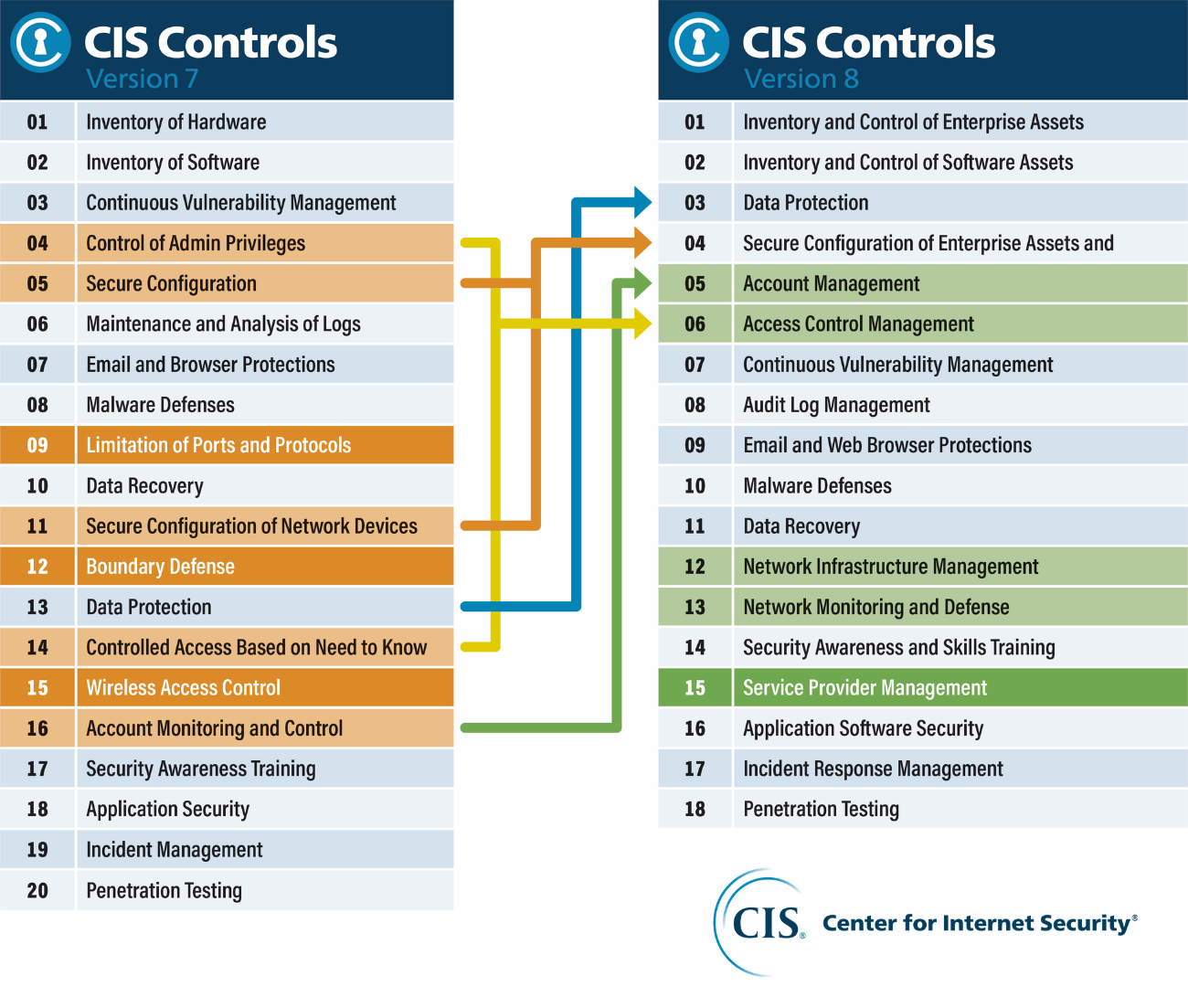
* **Risk Impact:**

For businesses, technology risk is governed by one equation: Risk = Likelihood x Impact. This means that the total amount of risk exposure is the probability of an unfortunate event occurring, multiplied by the potential impact or damage incurred by the event.

The formula is: **risk** = (threat x vulnerability x probability of occurrence x impact)/controls in place.

* **SANS CIS Controls:**

The CIS Controls (formerly known as Critical Security Controls) are a recommended set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive and dangerous attacks. SANS supports the CIS Controls with training, research, and certification.



* **Cybersecurity policies**

Cybersecurity policies are important because cyberattacks and data breaches are potentially costly.

Such practices might include:

* Rules for using email encryption.
* Steps for accessing work applications remotely.
* Guidelines for creating and safeguarding passwords.
* Rules on use of social media.
* **Cybersecurity Procedures:**
* Business Continuity Requests
* Credit Card Processing Procedures
* Data Privacy Procedures
* Patch Management Procedure
* Third Party Security Procedures
* Export Control (ITAR, EAR, etc.)
* Incident Response Procedure
* Vulnerability Management Procedure
* Policy Exception Procedure
* PCI DSS Assessment Procedure
* DFARS 7012 System Security Plan (SSP) and Assessment Procedure

* **Cybersecurity Standards:**
* Approved Endpoint Software
* Data Protection Safeguards
* Data Protection Safeguards - Cloud Computing
* Data Protection Safeguards - Endpoints
* Data Protection Safeguards - Mobile Devices
* Data Protection Safeguards - Servers
* Data Categorization
* Encryption Standard
* Network Firewall Standards
* Terms of Use (login banner)
* SSH Server Standard
* Email Standard
* Web Server Standard