Index:

- Apexaiq score
- IT asset management
- Vulnerabilities
- Obsolescence
- Compliance
- Maintenance
- End of Life, End of Support, End of Maintenance
- Asset Hygiene
- Crown Jewel
- Inventory
- NVD
- Patch Management
- Data Breaches
- MSP
- Device Types
- True Saas
- Inbound/Outbound Integration
- Compliance Standards - eg. CISA, CISO, HIPPA, ISO 27001
- Perimeter
- ROI (Return on Investment), KPI (Key Performance Indicators)
- Auto-remidiation
- Network protocols
- Due-diligence
- SOAR (Security Orchestration, Automation, and Response)
- Role of ITAM in Zero Trust Security Models
- Cyber Asset Attack Surface Management (CAASM)

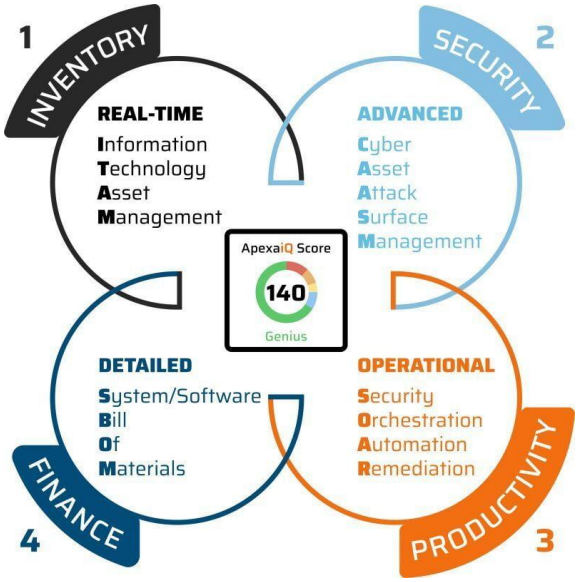
Apexaiq score:

ApexaiQ is a SaaS based platform that delivers your IT Risk Score, asset Compliance, Obsolescence, Maintenance and Vulnerability in a single dashboard.
In this dashboard, we give you a quantified and an actionable summary of your internal IT. This score, your Apexa iQ, is inspired by human IQ and ranges between 60 (poor) to 160 (genius).
Your Apexa iQ is like a credit rating for your entire IT estate, including every device on your network. It computes all your risks and security gaps into a single score, based on the most vital obsolescence and compliance factors. The higher the score, the stronger and more secure your IT environment.

THE SCORE IS CALCULATED BASED ON 3 DIFFERENT THINGS

1. IT Environment
2. Asset Hygiene - Obsolescence, Maintenance, Vulnerabilities
3. IT Gaps

Source: https://www.apexaiq.com/welcome-to-apexaiq/



IT asset management:

IT asset management (ITAM) is the end-to-end tracking and management of IT assets to ensure that every asset is properly used, maintained, upgraded and disposed of at the end of its lifecycle.

ITAM involves using financial, contractual and inventory data to track and make strategic decisions about IT assets. The main objective is to ensure that IT resources are used efficiently and effectively. ITAM also helps optimize costs by reducing the total number of assets in use and extending the life of those assets, avoiding costly upgrades. An important part of ITAM is understanding the total cost of ownership and finding ways to optimize asset use.

Source: https://www.ibm.com/think/topics/it-asset-management

Vulnerabilities:

Vulnerabilities are weaknesses in a system that gives threats the opportunity to compromise assets. Cyber security vulnerabilities are weaknesses in an organization's technological system that an attacker can use to infiltrate, steal data, or shut down an organization. Vulnerabilities mostly happened because of Hardware, Software, Network and Procedural vulnerabilities.

1. Hardware Vulnerability:
A hardware vulnerability is a weakness which can used to attack the system hardware through physically or remotely.
For examples:

1. Old version of systems or devices
2. Unprotected storage
3. Unencrypted devices, etc.

2. Software Vulnerability:
A software error happen in development or configuration such as the execution of it can violate the security policy. For examples:

1. Lack of input validation
2. Unverified uploads
3. Cross-site scripting
4. Unencrypted data, etc.

3. Network Vulnerability:
A weakness happen in network which can be hardware or software.
For examples:

1. Unprotected communication
2. Malware or malicious software (e.g.:Viruses, Keyloggers, Worms, etc)

3. Social engineering attacks
4. Misconfigured firewalls

4. Procedural Vulnerability:
A weakness happen in an organization operational methods.
For examples:

1. Password procedure – Password should follow the standard password policy.
2. Training procedure – Employees must know which actions should be taken and what to do to handle the security. Employees must never be asked for user credentials online. Make the employees know social engineering and phishing threats.

Source: https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-vulnerabilities/

https://www.geeksforgeeks.org/vulnerabilities-in-information-security/

Obsolescence:

Obsolescence is the process of becoming antiquated, out of date, old-fashioned, no longer in general use, or no longer useful, or the condition of being in such a state.

Outdated interfaces. Technology obsolescence occurs when hardware and software have been superseded by more advanced versions.

Source- https://www.pcmag.com/encyclopedia/term/technology-obsolescence

Technological obsolescence is the process by which existing technology, whether hardware or software, becomes less useful or efficient over time, losing its relevance or ability to meet current demands due to technological advancements, changes in industry standards, or the introduction of new and more advanced solutions.

This phenomenon can be attributed to various reasons, such as the evolution of industry standards, the emergence of disruptive technologies, lack of support or updates, and planned obsolescence by manufacturers to encourage the adoption of newer versions.

Source- https://genexus.blog/en_US/software-development/the-cost-of-technological-obsolescence/

Compliance:

IT compliance guidelines developed by regulatory bodies for engineering and designing infrastructure must be followed by developers and operations professionals. These guidelines determine the compliance and security measures that protect infrastructure by safeguarding consumer data. Every business should adhere to compliance guidelines that oversee their stored data to ensure that they are not in violation. Organizations face hefty fines for compliance violations, especially after a data breach.

Source: https://www.proofpoint.com/us/threat-reference/it-compliance

compliance is when businesses meet all the legal requirements, standards and regulations for the software their company uses to safeguard customer data. Achieving these standards means following all industry regulations, government policies, security frameworks and customer terms of agreement to ensure software security and appropriate usage in business.

Source: https://www.indeed.com/career-advice/career-development/it-compliance

Maintenance:

Software maintenance is any type of activity related to the optimisation of a software product. It plays a crucial role in the software development life cycle, ensuring the software remains up-to-date, enhances performance, and meets changing market demands. Some argue that it's a post-launch process, but without thinking about aspects of software maintenance such as hosting, infrastructure and disaster recovery, your project cannot be successful in the longer term.

Software maintenance is not only about fixing bugs, it's also about continuous honing of your product and making sure it performs at a level where it can provide the most value for its users. In the context of software engineering, it involves planned and unplanned activities to keep the system reliable and up-to-date.

Source: https://spyro-soft.com/blog/managed-services/what-is-software-maintenance-and-why-it-is-essential

End of Life:

End-of-Life (EoL) refers to the **point in a product's lifecycle when it no longer receives support or updates from the manufacturer**.

After this phase, the product is considered obsolete, meaning it won't have new features, bug fixes, security updates, or customer support.

EoL is a critical milestone in a product's lifecycle, signaling to users that they should start planning to upgrade or replace the product.

Recognizing the EoL is crucial for obsolescence risk management, as it helps organizations plan for upgrades or replacements to avoid potential operational and security risks.

End of Support:

End-of-Support (EoS), also known as End-of-Service Life (EoSL), **marks a specific point in a product's lifecycle when the manufacturer stops providing technical support**, including bug fixes, patches, and updates.

Unlike End-of-Life (EoL), which signifies the complete cessation of product support and updates, EoS indicates that while the product may still function, it will no longer receive the manufacturer's direct support or security updates, making it potentially vulnerable and less reliable over time.

Source: https://www.leanix.net/en/wiki/trm/what-is-end-of-life-vs-end-of-support

End of Maintenance:

End of Maintenance (EOM) refers to **the point at which a vendor will no longer provide updates or patches for a specific version of a product**. After this date, the product will continue to operate, but support will be limited to the version that is currently available, and no further maintenance releases will be provided for that version.

Asset Hygiene:

Asset hygiene in the context of IT and cybersecurity refers to **the ongoing process of ensuring that all assets within an organization adhere to security policies and best practices**. This includes maintaining up-to-date software, ensuring proper management and security of assets, and addressing vulnerabilities. It is crucial for maintaining the health and security of an organization's IT environment, similar to how personal hygiene is important for individual health.

Source: Google

Crown Jewel:

The crown jewels are a company's most prized and valuable assets.

The crown jewels may be physical assets or intangibles like patents or intellectual property and trade secrets.

The crown jewel defense is a hostile takeover defense that involves the sale of the target firm's crown jewels to make it less desirable to the acquirer.

Source: https://www.investopedia.com/terms/c/crownjewels.asp

Inventory:

IT asset inventory is the process of identifying, tracking, and managing all **hardware and software assets** an organization owns or uses. This includes servers, laptops, mobile devices, printers, network devices, software licenses, and other technology-related items contributing to the organization's **IT infrastructure**.

It's important to note that the **scope of IT asset inventory** goes beyond simply identifying IT assets; it involves managing **assets through their entire lifecycle**, from acquisition to retirement.

Source: https://blog.invgate.com/it-asset-inventory

NVD:

The **National Vulnerability Database** (**NVD**) is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics.

Source: https://en.wikipedia.org/wiki/National_Vulnerability_Database

Patch Management:

Patch management is the process of distributing and applying updates to software. These patches are often necessary to correct errors (also referred to as “vulnerabilities” or “bugs”) in the software. Common areas that will need patches include operating systems, applications, and embedded systems (like network equipment). When a vulnerability is found after the release of a piece of software, a patch can be used to fix it. Doing so helps ensure that assets in your environment are not susceptible to exploitation.

Source: https://www.rapid7.com/fundamentals/patch-management/

Data Breaches:

A data breach is the release of confidential, private, or otherwise sensitive information into an unsecured environment. A data breach can occur accidentally, or as the result of a deliberate attack.

Major corporations are prime targets for attackers attempting to cause data breaches because they offer such a large payload. This payload can include millions of users' personal and financial information, such as login credentials and credit card numbers. This data can all be resold on underground markets.

However, attackers target anyone and everyone they can extract data from. All personal or confidential data is valuable to cyber criminals — usually, someone in the world is willing to pay for it.

Source: https://www.cloudflare.com/learning/security/what-is-a-data-breach/

MSP:

A managed service provider (MSP) is a third-party company that remotely manages a customer's information technology (IT) infrastructure and end-user systems. Small and medium-sized businesses (SMBs), nonprofits and government agencies hire MSPs to perform a defined set of day-to-day management services. These services may include network and infrastructure management, security and monitoring.

Source: https://www.techtarget.com/searchitchannel/definition/managed-service-provider

Device Types:

Device types define information about a class of devices, including properties that apply to all devices of a type. Properties defined for a device type can be overridden for an individual device.

Source: https://docs.oracle.com/en/industries/energy-water/smart-grid-gateway/2.5.0.0.0/sgg-user-guides/index.html#page/SGG_25000/D1_AG_Understanding_Device_Types.html

True Saas:

True SaaS (Software as a Service) is **a cloud-based software distribution model where a third-party provider hosts and maintains the servers, databases, and code that constitute an application**. This model allows for continuous innovation, security, agility, and scalability. True SaaS solutions are hosted entirely in the cloud and managed by the service provider, which includes regular system upgrades, security patches, and compliance checks, all bundled into a single contract with contractual Service Level Agreements (SLAs).

Inbound/Outbound Integration:

Inbound and outbound integration in ApexAIQ refers to **the processes of receiving and sending data between systems**. Inbound integration involves external systems sending data to ApexAIQ, while outbound integration involves ApexAIQ sending data to external systems. These integrations enable seamless communication and data exchange, enhancing operational efficiency and customer experience.23

In an inbound scenario, an external system might send data to ApexAIQ, which then processes and acknowledges the request. Conversely, in an outbound scenario, ApexAIQ might send data to an external system, such as creating a similar record in a third-party tool when an incident is created in ApexAIQ.

Compliance Standards - eg. CISA, CISO, HIPPA, ISO 27001:

HIPAA – Health Insurance Portability and Accountability Act

HIPAA or the Health Insurance Portability and Accountability Act is a federal law that mandates the creation of national standards to protect sensitive patient data from being disclosed without the consent of the patient.

ISO 27001 – International Standard on requirements for information security management

ISO 27001 is a standard for managing and implementing Information Security Management Systems or ISMS. It provides a comprehensive framework for organizations to manage and protect sensitive data and information.

CISA -Certified Information Systems Auditor

Compliance standards in the context of information security and technology governance refer to **the policies and guidelines that organizations must follow to ensure the protection and secure handling of information**. These standards are crucial for maintaining regulatory

compliance and protecting against security threats. For example, the CISA (Certified Information Systems Auditor) certification validates expertise in auditing, control, and security in information systems, focusing on assessing vulnerabilities, maintaining compliance, and implementing controls within an organization's IT infrastructure.34

CISO -Chief Information Security Officer

The role of a CISO (Chief Information Security Officer) involves directing staff in identifying, developing, implementing, and maintaining processes to reduce information and IT risks. A CISO is responsible for establishing and maintaining enterprise vision, strategy, and programs to ensure information assets and technologies are adequately protected.

Source: https://sprinto.com/blog/compliance-standards/

Perimeter:

software-defined perimeter(SDP), which is a method of enhancing computer security by controlling access to resources based on identity.13

An SDP framework was developed by the Cloud Security Alliance to ensure that both device posture and identity are verified before granting access to application infrastructure. This approach follows a need-to-know model, where connectivity is established only for authorized users and resources.

ROI (Return on Investment):

Return on investment (ROI) is a performance measure used to evaluate the efficiency or profitability of an investment or compare the efficiency of a number of different investments. ROI tries to directly measure the amount of return on a particular investment, relative to the investment's cost. Key factors influencing ROI include the initial investment amount, ongoing maintenance costs, and the cash flow generated by the investment.

To calculate ROI, the benefit (or return) of an investment is divided by the cost of the investment. The result is expressed as a percentage or a ratio.

Source: https://www.investopedia.com/terms/r/returnoninvestment.asp

KPI (Key Performance Indicators):

Key Performance Indicators (KPIs) are the critical (key) quantifiable indicators of progress toward an intended result. KPIs provide a focus for strategic and operational improvement, create an analytical basis for decision making and help focus attention on what matters most.

Source: https://www.kpi.org/kpi-basics/

Auto-remidiation:

Automated data remediation is a process that leverages technology to identify and correct noncompliant data. This process helps organizations mitigate the risk of financial loss and reputational damage by swiftly detecting and managing vulnerabilities.

Data remediation involves organizing, cleansing, and migrating data to ensure it is protected and serves its intended purpose. Tasks such as data cleansing, data validation, and data profiling are integral to this process.

Network Protocols:

Network protocols are a set of rules that are responsible for the communication of data between various devices in the network. These protocols define guidelines and conventions for transmitting and receiving data, ensuring efficient and reliable data communication.

- **Transmission Control Protocol (TCP)**: Ensures reliable data transmission by managing packet loss and ensuring correct delivery.567
- **Internet Protocol (IP)**: Manages the addressing of packets to ensure they reach their destination.567
- **User Datagram Protocol (UDP)**: Provides a faster, connectionless service for streaming or gaming but lacks error correction.567
- **Hypertext Transfer Protocol (HTTP)**: Used for web browsing, defining how messages are formatted and transmitted.567
- **Hypertext Transfer Protocol Secure (HTTPS)**: An extension of HTTP that includes security protocols like SSL/TLS for encryption and authentication.68
- **File Transfer Protocol (FTP)**: One of the most commonly used file transfer protocols on the Internet and within private networks.27
- **Network Time Protocol (NTP)**: Used to synchronize the devices on the Internet, ensuring precise clocks across devices.2
- **Internet Protocol version 4 (IPv4)**: The most popular version of the Internet Protocol, responsible for distributing data packets throughout the network.8
- **Internet Protocol version 6 (IPv6)**: The most recent version of the Internet Protocol, created to address the drawbacks of IPv4.

Source: https://www.geeksforgeeks.org/types-of-network-protocols-and-their-uses/

Due-diligence:

Due diligence is a systematic way to analyze and mitigate risk from a business or investment decision.

An individual investor can conduct due diligence on any stock using readily available public information.

The same due diligence strategy will work on many other types of investments.

Due diligence involves examining a company's numbers, comparing the numbers over time, and benchmarking them against competitors.

Due diligence is applied in many other contexts, for example, conducting a background check on a potential employee or reading product reviews.

Source: https://www.investopedia.com/terms/d/duediligence.asp

SOAR (Security Orchestration, Automation, and Response):

Security orchestration, automation and response (SOAR) technology helps coordinate, execute and automate tasks between various people and tools all within a single platform. This allows organizations to not only quickly respond to cybersecurity attacks but also observe, understand and prevent future incidents, thus improving their overall security posture.

Source: https://www.paloaltonetworks.com/cyberpedia/what-is-soar

Role of ITAM in Zero Trust Security Models:

Zero Trust is a cybersecurity strategy based on eliminating any trust within an environment regardless of location. Everyone and everything is read as a threat until proven otherwise. All users and devices must be authenticated and authorized before being allowed access to valuable resources.

Doubt

Cyber Asset Attack Surface Management (CAASM):

Cyber asset attack surface management (CAASM) is a platform tool that leverages data integration, conversion, and analytics to provide a unified view of all physical and digital cyber assets that comprise an enterprise network.

CAASM can be integrated with existing workflows to automate security control gap analysis, prioritization, and remediation, thereby boosting efficiency and breaking down operational silos between teams and their tools. It's important to remember, however, that the assets these tools are meant to protect are more than just devices and infrastructure.

Source: https://www.rapid7.com/fundamentals/what-is-cyber-asset-attack-surface-management-caasm/