

How comprehensive hardware asset management helps ensure compliance with new NIS2 regulations

Organisations across the 27-member European Union are rushing to meet an October 17 deadline to comply with a new set of rules aimed at **strengthening and focusing cybersecurity best practices**. The Network and Information Systems Security Directive 2 (NIS2) elements are grounded in sound IT asset lifecycle management principles.

NIS2 is an extension of the original NIS Directive of 2016 that adds specificity and accounts for vulnerabilities that emerged during the COVID-19 pandemic. It expands coverage to more organisations and distinguishes “essential” and “important” entities.

Essential entities provide services fundamental to public health, security, and commerce. They include energy suppliers, transportation providers, financial

services firms and healthcare providers. Important entities deliver less critical services that are still necessary for economic and social health. Both are subject to NIS2 rules, although the penalties differ somewhat by organisation type. Organisations outside of the EU that do business within EU borders are subject to the new rules.



Essential entities (EE)



Energy



Transport



Finance



Public
administration



Health



Space



Water supply
(drinking & wastewater)



Digital
infrastructure

Important entities (IE)



Postal services



Waste
management



Chemicals



Research



Foods



Manufacturing



Digital providers

The intersection of cybersecurity and hardware asset management (HAM)

Cybersecurity asset management (CSAM) is the process of discovering, maintaining an inventory of, monitoring, managing and tracking an organisation's assets, including hardware, software, data and cloud-based services, to determine what those assets do and identify any gaps in its cybersecurity protections. For IT hardware, such as endpoint devices and on-premises IT infrastructure, this involves understanding the value, location, and vulnerability of each asset.

IT asset lifecycle management is a cradle to grave approach to managing the entire lifecycle of an organisation's IT hardware assets, maximising use while minimising costs and risks.

By strengthening IT asset lifecycle management processes, organisations can improve compliance and their overall cybersecurity posture. Having a clear plan with a strategy in place before you begin is a clear first step. Here are where the directive's rule and asset lifecycle management intersect.

1. Supply chain security: Mitigating third-party risks

The pandemic exposed many serious gaps in supply chain security. Some organisations discovered they did not know all the players in their supply chains and had little insight into their security practices.

NIS2 requirement: Organisations must assess the cybersecurity risks their suppliers and service providers pose. This includes evaluating their security practices, incident response protocols, and system vulnerabilities. Entities must implement rigorous security protocols that cover all aspects of their interactions with suppliers, conduct thorough risk assessments and audits to evaluate suppliers' security measures and ensure that these measures align with their own security standards.

Organisations **must** assess the cybersecurity risks their suppliers and service providers pose

Asset Lifecycle Management best practice:

Implement vendor risk management protocols during the procurement phase and periodically review vendor practices to ensure adherence to the buyer's security protocols. Contracts should specify security measures suppliers must take and outline data protection and incident reporting expectations. Suppliers must agree to periodic audits to ensure compliance. Particular care should be taken to understand what kind of certifications and accreditations the vendor has which provides validation from a third party that the services being provided are up to standards. Examples include NAID AAA certification from i-SIGMA, ISO 9001, and ADISA.

Alignment: A robust asset lifecycle management strategy naturally integrates supply chain security. It begins with conducting a supply chain risk assessment and gathering information about third-party partners' chain of custody. Rules are created for vetting vendors, including security considerations throughout the contracting and procurement process and response strategies in case of a breach or disruption. Continuous monitoring and testing significantly reduce the risk of vulnerabilities entering systems.

2. Secure acquisition, development, and maintenance of IT assets

NIS2 requirement: Organisations must implement measures to ensure the security of network and information systems throughout their lifecycle, from acquisition to development, deployment, and maintenance.

Asset Lifecycle Management best practice: Asset lifecycle management prioritises data security throughout the asset lifecycle, from securely storing, deploying and retrieving equipment to data wiping, redeployment and secure end-of-use processes. This includes procedures for regulating access to storage areas, ensuring that assets are inspected for vulnerabilities before deployment, tagging and tracking of assets in use, following a rigorous process for applying patches and updates and sanitising equipment designated for disposal or reuse. An important element underscoring the movement of the assets is providing a tracking and real-time reporting capability. Data security and accountability for the asset should be provided with tracking and reporting that supports decision making as well compliance requirements.

Alignment: Asset lifecycle management enforces cybersecurity practices that meet all the NIS2 requirements. It also requires the preparation of an incident response plan outlining procedures for addressing vulnerabilities promptly and responding to disruptions.

3. Basic cyber hygiene and cybersecurity training

NIS2 requirement: Organisations must implement appropriate technical and organisational measures to manage cybersecurity risks, including basic cyber hygiene practices and employee training programs tailored to specific roles and responsibilities.

Asset Lifecycle Management best practice: End users should be trained in best practices for safe and secure handling of corporate IT equipment, such as not leaving assets unattended and protocols for returning corporate IT equipment. IT staff managing corporate assets should be trained on organisational mandates for certified data sanitisation between deployments and during end-of-life disposition. The IT organisation should maintain a master inventory of all assets, status and location, and compliance with preventive measures. There are two common approaches to the inventory audit which include the 'wall to wall' approach which is a large expansive effort to identify all assets at one time. An alternative method is the 'rolling' approach which audits assets in distinct projects and areas, and is more practical for larger organisations. In either case, it's crucial to have an ongoing effort to have a physical audit of IT assets for security and asset management purposes.

Alignment: A strong asset lifecycle management strategy incorporates the human element in cybersecurity, assuming most breaches are caused by human error. Training employees in best practices empowers them to become the first line of defense against cyber threats. Corporate mandates requiring certified data sanitisation of assets ensure cyber security at end-of-use.

It's crucial to have an ongoing effort to have a physical audit of IT assets



4. Risk management and business continuity

NIS2 requirement: Risk management is fundamental to the new directive. Management teams must master the discipline of risk assessment and implement measures to minimise risks in ongoing operations. These include the three measures outlined above, and established processes for documenting and reporting major incidents within 24 hours. A business continuity plan must be created to ensure continued operations, even during major incidents.

Asset Lifecycle Management best practice:

Asset lifecycle management is grounded in risk management. Procedures and policies are created and priorities set based on the assessed risk to the organisation. The risks of acquiring and implementing assets are incorporated in the procurement process. Risk assessments help determine the frequency and depth of maintenance activities. Upgrades, modifications and retirement of aging equipment are informed, in part, by perceived risk. From a risk management perspective it is critical to ensure data is not only sanitised, but a certificate of data sanitisation (COD) is provided when assets are being resold to recover some of their value. Value recovery through reselling assets is an important part of optimising the value of the asset, but simultaneously, there needs to be assurance that the data from the first owner has been completely sanitised and verified which is what the COD provides.

Alignment: The risk management principles incorporated into asset lifecycle management best practices align directly with the requirements laid out in NIS2.



Final thoughts

NIS2 and asset lifecycle management share the common goal of enhancing organisational cybersecurity as it relates to the tracking, handling and disposition of IT hardware assets. Organisations that adhere to sound hardware asset management practices are not only in a better position to comply with the regulations but also to protect IT infrastructure, data, and operations. A well-defined asset lifecycle management strategy that prioritises supply chain visibility, secure acquisition and configuration practices, and responsible disposal of IT assets is a cornerstone of effective cybersecurity in the age of NIS2.

+44 (0) 1782 654 710 | ironmountain.com/en-gb

R.O.I. 1800 732 673 | N.I. +44 (0) 1782 654 710 | ironmountain.com/en-ie

About Iron Mountain

Iron Mountain Incorporated (NYSE: IRM), founded in 1951, is the global leader for storage and information management services. Trusted by more than 220,000 organisations around the world, and with a real estate network of more than 85 million square feet across more than 1,400 facilities in over 50 countries, Iron Mountain stores and protects billions of information assets, including critical business information, highly sensitive data, and cultural and historical artifacts. Providing solutions that include secure storage, information management, digital transformation, secure destruction, as well as data centres, art storage and logistics, and cloud services, Iron Mountain helps organisations to lower cost and risk, comply with regulations, recover from disaster, and enable a more digital way of working. Visit www.ironmountain.com/en-gb for more information.

© 2023 Iron Mountain, Incorporated and/or its affiliates ("Iron Mountain"). All rights reserved. Information herein is proprietary and confidential to Iron Mountain and/or its licensors, does not represent or imply an invitation or offer, and may not be used for competitive analysis or building a competitive product or otherwise reproduced without Iron Mountain's written permission. Iron Mountain does not provide a commitment to any regional or future availability and does not represent an affiliation with or endorsement by any other party. Iron Mountain shall not be liable for any direct, indirect, consequential, punitive, special, or incidental damages arising out of the use or inability to use the information, which is subject to change, provided AS-IS with no representations or warranties with respect to the accuracy or completeness of the information provided or fitness for a particular purpose. "Iron Mountain" is a registered trademark of Iron Mountain in the United States and other countries, and Iron Mountain, the Iron Mountain logo, and combinations thereof, and other marks marked by ® or TM are trademarks of Iron Mountain. All other trademarks may be trademarks of their respective owners.