End-of-Life (EOL) Management:
Questions Board Members Should Ask

Below are some questions you may ask management to ensure end-of-life (EOL) management practices has been appropriately implemented to protect against cyber threats.

1. ***Does the institution have processes in place to maintain a comprehensive and ongoing inventory of all hardware and software assets within the institution, including all assets that are not in regular use but may be deployed at any time on the institution's network?***

   WHY THIS IS IMPORTANT: Tracking all institutional hardware and software assets can be a daunting task, especially in larger institutions. However, it is vitally important that the institution have a process in place to identify and track assets to ensure they are included as part of the institution's ongoing vulnerability and patch management programs and, in the context of end-of-life management, that they are identifiable to afford the institution sufficient time to plan for their retirement by the vendor. The institution simply cannot manage or apply adequate security protections to assets it does not know it has.

2. ***Does the institution's asset identification process:***
   a. ***Identify vendor-reported retirement or sunset dates for all hardware and software assets, and***
   b. ***Include the identification of asset interdependencies to avoid potential conflicts or operational issues once the asset is retired or replaced?***

   WHY THIS IS IMPORTANT: Vendors typically announce the sunsetting of hardware and software assets with enough lead time to allow the institution to plan for their retirement, replacement, or the engagement of service contracts to support the asset past its sunset date. But simply identifying the asset's retirement date is likely not enough; proper end-of-life management ensures that plans for addressing a sunsetting asset also include the identification of any asset interdependencies and plans to address any potential operational issues with enough lead time to ensure that conflicts with other assets or processes are avoided to the extent possible.

3. ***Does the institution currently utilize any unsupported or out-of-date hardware or software assets? If so, are satisfactory compensating controls in place to reduce the risk associated with the continued use of these assets? Does the institution have an active plan to replace these unsupported or out-of-date assets?***

- *WHY THIS IS IMPORTANT: Unpatched or outdated technology opens the door to easily exploitable and frequently targeted vulnerabilities. This can lead to unauthorized access to information, data breaches, and the introduction of malware. The continued use of end-of-life assets or outdated technology in the technology environment may also lead to compatibility issues with other technologies in the institution. Future upgrades or replacements of other technologies may conflict with unsupported legacy hardware and software, creating conflicts, limiting modernization efforts, or affecting usability and security of existing technologies. Finally, unsupported technology can*

lead to Increased costs associated with maintaining outdated software, addressing usability conflicts, and potential reductions in system performance, security, or reliability.

4. ***Does the institution have a written policy in place to document the institution's end-of-life management strategy and processes, including:***
    a. ***Replacing or retiring sunsetting assets and complying with institution requirements for implementing new systems or applications;***
    b. ***Identification of the risks of operating unsupported assets and guidance for implementing compensating controls for any assets that must be kept beyond their sunset date, including isolating or segregating the asset from the network, adjusting existing security configurations, and/or acquiring extended vendor service agreements, as necessary, to extend support for sunsetting assets;***
    c. ***Conducting risk assessments on systems and applications to identify potential vulnerabilities, upgrade opportunities, or new defense layers, and to help determine end-of-life; and***
    d. ***Specific procedures for the secure destruction or data wiping of hard drives returned to vendors or donated, to prevent the inadvertent disclosure of sensitive information?***

WHY THIS IS IMPORTANT: Management of end-of-life assets is a somewhat complex process that requires a forward looking, organized approach. A comprehensive end-of-life management policy provides structure for the institution's management of end-of-life assets, covering general asset identification and management strategies, as well as identification and management of the various risks associated with end-of-life assets.