How Do Blancco Erasure Solutions Help Organizations Comply with the Saudi Arabian Monetary Authority (SAMA) Cyber Security Framework?

In May 2017, the Saudi Arabian Monetary Authority released its Cyber Security Framework to guide organizations in the region on how to best avoid cyber security threats and deal with threats as they occur. Regulated industries in Saudi Arabia such as banking, insurance and finance, are listed as a top concern in the framework.

Section 3.3.11 of the framework, "Secure Disposal of Information Assets," outlines how organizations should securely dispose of information assets when they are no longer required. The objective of this section, as outlined in the document, is '[t]o ensure that the Member Organization's business, customer and other sensitive information are protected from leakage or unauthorized disclosure when disposed."

Blancco erasure solutions help organizations comply with this framework in the following ways:

Control Considerations (SAMA Framework)	How Blancco Data Erasure Helps
"Information assets should be disposed in accordance with legal and regulatory requirements, when no longer required (i.e. meeting data privacy regulations to avoid unauthorized access and avoid (un)intended data leakage)."	Blancco Data Erasure solutions securely and irreversibly erase data from a wide array of IT assets, including servers, LUNs, hard drives, SSDs, laptops, mobile phones and more. Data can be erased at any point during its lifecycle (active or inactive) when it's no longer required. This helps organizations avoid unauthorized access and unintended leakage.
"Sensitive information should be destroyed using techniques to make the information non-retrievable (e.g., secure erase, secure wiping, incineration, double crosscut, shredding)."	Blancco data erasure solutions achieve data sanitization by deliberately, permanently and irreversibly removing the data stored on memory devices to make it unrecoverable. Blancco does this through its three-step data erasure process: 1. Allow for selection of a specific standard, based on your industry and organization's unique needs. 2. Verify the overwriting methodology has been successful and removed data across the entire device, or target data (if specifically called). 3. Produce a tamper-proof certificate containing information that the erasure has been successful and written to all sectors of the device, along with data about the device and standard used.
"The Member Organization should ensure that third party service providers used for secure disposal, transport and storage comply with the secure disposal standard and procedure and the effectiveness is periodically measured and evaluated."	IT asset disposition vendors (ITADs) using Blancco's secure data erasure processes ensure complete data removal from IT assets before recycling, resale or destruction.

H3 Secure works with Blancco to distribute data erasure solutions that support compliance with cyber security guidance such as SAMA. Contact us today for additional information about how we can help you pass your next data or cyber security audit.

H3Secure

For more information, please visit www.h3secure.com or call +971 4 333 8499.