blancco

How Blancco Helps Organizations Comply with Philippines Central Bank Circular 982 (BSP Circular 982)

Cyberthreats pose an increasing risk to financial services organizations worldwide, including those in the Philippines. To strengthen the security posture of Bangko Sentral supervised financial institutions (BSFIs), Bangko Sentral ng Pilipinas, the Central Bank of the Philippines, issued Circular No. 982 in late 2017. Since the designated year for coming into compliance has now passed, BSFIs are being held accountable for implementing the Circular's enhanced guidelines on information security management.

What is a Cyberthreat?

Circular 982 defines a cyberthreat (or, "cyberattack," "cyber fraud" or "cyber-related incident") to be "a deliberate act of omission or commission by any person carried out using the internet and/or other electronic channels, in order to communicate false or fraudulent representations to prospective victims, to conduct fraudulent transactions, **or to illegally obtain proprietary data or information related to the institution, their customers and other stakeholders**." [Emphasis added.]

For financial institutions and other organizations, this proprietary content includes sensitive data being actively used for carrying out business. It also includes data that is being transferred from one device to another or data that has reached the end of its retention period or usefulness. In either instance, confidential data can be vulnerable without proper data erasure processes in place.

How Does Circular 982 Affect Philippine BSFIs?

Under the new regulation, BSFIs must report major cyber-related incidents and financial services and operations disruptions within two hours of discovery. BSFIs are also directed to protect information throughout its lifecycle, from handling, storage (data at rest), transmission (data in transit) and up to the disposal phase.

Circular 982 guidelines also intersect with other data privacy and protection regulations, including The Law on Secrecy of Bank Deposits, the Data Privacy Act of 2012 and the requirements of the Payment Card Industry Data Security Standard (PCI DSS). Data erasure plays a critical role within each of these data protection mandates.

The Role of Data Erasure in Philippine Information Security Management

A robust data sanitization program limits the amount of data that can be exposed during a breach and enables compliance with complementary financial privacy and security regulations.

The following table shows how integrating Blancco data erasure solutions could fit within your institution's information security program (ISP) and information security strategic plan (ISSP) to ensure compliance with Circular 982.

Circular No. 982 Highlights

RELEVANT PRINCIPLES FROM FROM CIRCULAR 982	HOW BLANCCO HELPS
Annex A, Appendix 75b/ Appendix Q-59b: **2.6. Compliance with Relevant Laws, Regulations and Standards.** In designing the ISSP and ISP, compliance with relevant laws, regulations, and standards must be fully considered. For BSFIs, these include The Law on Secrecy of Bank Deposits under R.A. No. 1405 and recently, the Data Privacy Act of 2012 under R.A. No. 10173. For BSFIs that process and issue payment cards under international brand schemes (e.g., VISA, Mastercard, AMEX, etc.), the ISP should be tailored to fit the requirements of the Payment Card Industry Data Security Standard (PCI DSS). Moreover, Management may find having security certifications such as those provided by the International Organization for Standardization (ISO) and other certifying bodies to be of significant value to the business.	Blancco has extensive experience meeting secure data erasure requirements for highly regulated industries. Our ability to meet stringent erasure standards helps Philippine BSFIs meet Circular 982's requirement to comply with relevant laws, regulations and standards when it comes to securely and completely erasing confidential data at data or asset end-of-life: • Blancco Drive Eraser, Blancco File Eraser, and Blancco Management Console each address various critical data disposal, right to erasure, and personal information protection elements of Philippines Data Privacy Act Rule IV; Rule VIII; and Rule IV. • Blancco erasure solutions also address PCI DSS elements within Requirements 3 (Protect Stored Cardholder Data), 9 (Restrict Physical Access to Cardholder Data), and 10 (Track and Monitor Network Access). Blancco also has two ISO certifications. ISO27001 certifies that Blancco's core functions meet specific requirements for a quality information security management system. In addition, Blancco Data Eraser solutions completely and permanently remove data from LUNs, virtual machines, removable media, drives, computers and mobile devices before they are recycled, reused or resold, helping client organizations meet ISO 27001 requirements. ISO9001 demonstrates our ability to consistently provide products and services that meet customer and applicable statutory and regulatory requirements. These ISO certifications allow Blancco to advise on best practices for complying with applicable data sanitization standards.
Annex A, Appendix 75b/ Appendix Q-59b: **3.3.2. Physical and Environmental Controls.** Physical security measures should be in place to protect computer facilities and equipment from damage or unauthorized access that can impair the confidentiality, integrity, and availability of information... **Moreover, a specific and formal authorization process should be employed for the removal of hardware and software from the premises.** [Emphasis added]	The process of removing hardware and software from an organization's premises should include complete and secure data erasure to protect the confidentiality of that data. This ensures that sensitive business or personal data is not vulnerable to unauthorized access when storage media leaves the site for decommissioning or maintenance. Blancco erasure solutions securely and completely erase hard disk drives (HDDs), solid-state drives (SSDs), USB and SD storage media and more, from mobile devices to servers, before they leave your secure environment. Erasure can target individual files, a fleet of workstations or entire data centers. Furthermore, each erasure comes with a tamper-proof certificate of erasure and provides an audit trail that verifies data erasure has occurred before storage assets leave the organization's protection.

RELEVANT PRINCIPLES FROM FROM CIRCULAR 982	HOW BLANCCO HELPS
Annex A, Appendix 75b/ Appendix Q-59b: 3.3.3.3.1. Virtualization. As BSFIs are increasingly leveraging on virtualization technologies to optimize existing hardware resources, reduce operating expenses and improve IT flexibility and agility to support business needs, additional security risks such as attacks on hypervisor integrity and lack of visibility over intra-host communications and virtual machine (VM) migrations are also rising. To address such risks, Management should extend security policies and standards to apply to virtualized servers and environment.	Virtual machines should be treated in the same way as physical servers to ensure there is no data left behind. Blancco Virtual Machine Eraser allows organizations to automatically destroy all data when virtual machines are no longer needed. With highly flexible deployment options, Philippine BSFIs can choose between erasing data from standalone and target-specific virtual machines with command lines on the hypervisor layer. Blancco Virtual Machine Eraser supports the greatest number of hypervisors across VMware ESXi, Microsoft Hyper-V, Oracle Virtual Box and virtual hard disk formatted for VMDK, VHDX, VDI and OVF. In addition, Blancco Virtual Machine Eraser integrates easily with VMware, produces a 100% certified and tamper-proof audit trail, and ensures compliance with industry standards and regulations, including PCI DSS, ISO 27001 and the EU's General Data Protection Regulation.
Annex A, Appendix 7Sb/Appendix Q-59b: 3.3.3.5.1. Data-at-Rest. (Computer Systems, Physical Media) Policies, standards, and procedures as well as risk management controls must be in place to secure the BSFI's information assets, whether stored on computer systems, physical media, or in hardcopy documents. The level of protective controls shall depend on the sensitivity and criticality of the information. Sensitive information such as system documentation, application source code, and production transaction data are expected to have more extensive controls to guard against alteration or data leakage (e.g., integrity checkers, cryptographic hashes, data leakage prevention systems). Management should likewise implement appropriate controls over information stored on portable devices such as laptops, smart phones, and tablets taking into account their susceptibility to lost or theft. Applicable risk mitigation controls include data encryption, host-provided access controls, homing beacons, and remote wiping or deletion capabilities, among others.	Blancco active erasure solutions, including Blancco File, Blancco LUN and Blancco Virtual Machine, securely erase data in active environments as it is no longer needed–increasing data erasure compliance, lessening downtime and lessening the impact on your business when a cyber breach does occur by limiting the attack surface. This can be done either manually or, to better ensure that data management policies are followed at end-of-life, set up to be conducted automatically according to specific parameters (e.g., by file type, date, or other configurations). • For PCs, laptops, and servers, Blancco File Eraser can securely erase sensitive files and folders • Blanco LUN Eraser allows organizations to erase data in active storage environments while allowing the operating system to remain intact. LUNs are immediately available for reuse after erasure. • Blancco Virtual Machine Eraser allows organizations to automatically destroy all data when virtual machines are no longer needed. In addition, Blancco Drive Eraser securely erases sensitive data from HDDs and complex SSDs in desktop/laptop computers and servers. All of these features help organizations reduce the amount of redundant, old, or trivial data that merely becomes a liability after it has outlived its usefulness or fulfilled its retention requirements.

Continued...

RELEVANT PRINCIPLES FROM FROM CIRCULAR 982	HOW BLANCCO HELPS
Annex A, Appendix 7Sb/Appendix Q-59b3.3.3.5.1. Data-at-Rest. (Cloud section) Considering the unique risk dimensions of storing data in cloud computing platforms, Management should fully understand the nature of the cloud technology in line with business requirements and satisfy themselves as to the level of security (e.g., how access is controlled and how information is retrieved) and compliance to data privacy and other relevant rules and regulations. Information security and accountability still rests with the institution's Management, hence, it should exercise effective oversight over the cloud service provider in terms of adherence to security, performance and uptime, and back-up and recovery arrangements contained in the contract/ agreement.	When it's time for data to be removed from physical or virtual storage in the cloud due to changing cloud providers, customer requests, or data retention obligations, Blancco helps you make sure your old BSFI data is truly erased from cloud servers. As a best practice, organizations should contractually require cloud vendors to provide an audit trail proving that organizational data is being managed properly, as well as certifiable proof that it has been securely erased at data end-of-life. After all, deleting old, obsolete and no longer needed data reduces cloud storage costs, supports compliance with data protection laws, and prevents excess data from becoming an access risk. Erase data yourself where applicable and permitted. If you rely on virtual disk drives and accessing data in a logical unit number (LUN) environment, Blancco LUN Eraser can ensure that data on the LUN has been securely overwritten. It is specifically built to erase virtual data stores from virtual servers hosted on public cloud platforms (e.g., AWS). LUN erasures come with a certificate of erasure stating which volume IDs have been erased, also helping to prove compliance and provide a tamper-proof audit trail.
Annex A, Appendix 75b/ Appendix Q-59b: 3.3.3.5.3. Removal, Transfers and Disposition of Assets. Procedures for the destruction and disposal of media containing sensitive information should be risk-based relative to the sensitivity of the information and the type of media used to store the information. Disposal techniques that the BSFI may implement include deletion, overwriting, degaussing [demagnetizing], and physical destruction of the media. **Management should be mindful about residual data being stored in computer-based media.** [Emphasis added]	Implementing the most appropriate methods of data destruction or erasure is critical when disposing of highly sensitive data (consider proprietary information, personally identifiable information, or other information with a high-risk of harm if accessed inappropriately). Choosing an inappropriate method can leave data behind. (See also, "Bank IT Security and False Positives for Secure SSD Erasure: What Your ITAD Vendor May Not Be Telling You.") Not all data destruction methods work in the same way or with the same efficacy for all media. (For instance, degaussing does not erase data from SSDs; deletion removes only the pointers to data—the data itself remains on the drive, where it's vulnerable to accidental exposure or theft.) Blancco's software-based data erasure solutions securely overwrite data from any data storage device using zeros and ones onto all sectors of the device. The number of overwriting passes, as well as whether additional firmware-based commands are implemented, depends on the device type and the erasure standard requested. Blancco solutions eliminate data with confidence from both magnetic and flash-based data storage media—including PCs, servers, mobile devices and removable media, as well as most PC-based ATMs—meeting the most rigorous data erasure standards. Additionally, all Blancco erasures come with a Certificate of Erasure and a 100% tamper-proof report.

Continued...

RELEVANT PRINCIPLES FROM FROM CIRCULAR 982	HOW BLANCCO HELPS
Annex A, Appendix 75b/ Appendix Q-59b: 3.3.3.8.4. Vendor Management and Outsourcing. ...Contracts should sufficiently detail information security requirements, particularly for TPSPs [third party service providers] that store, transmit, process, or dispose of customer information. Mechanisms should be in place to properly monitor the performance of third party service providers to confirm whether sufficient level of controls is maintained. Considering that TPSPs may be a source of cyber-risks, Management should properly assess cyber-risk exposures from TPSPs in order to proactively adjust their cyber-risk management programs.	Data transferred or shared with third-party organizations should be disposed of after the project is finished or after the business purpose is served. Blancco File Eraser helps financial institutions erase targeted files that should not be provided to third-party systems before an engagement. For data assets that are outsourced for recycling or other services where assets leave your organization's control, bulk erasure using Blancco data erasure solutions provide assurance that sensitive data has not been retained on IT assets. It is also recommended that BSFIs require TPSPs to contractually agree to securely erasing files after the engagement or any needed retention periods. Blancco can also advise clients on best pratices for third-party data erasure.
Annex A, Appendix 75b/Appendix Q-59b 3.4.1. Log Management. Log files can be analyzed for real-time or near real-time detection of anomalous activities, facilitate subsequent investigation of security incidents and can serve as forensic evidence for the prosecution of fraudulent activities. Thus, Management should put in place adequate security controls to prevent unauthorized access, modification and/or deletion of log files. Depending on the criticality of information..., Management should implement the following controls...: a. Encrypting log files containing sensitive data...; b. Ensuring adequate storage capacity ...; c. Restricting access and disallowing modification to log files...; and **d. Securing backup and disposal of log files.** [Emphasis added]	Disposing of log files that are no longer needed can be accomplished manually or automatically using Blancco File Eraser. By targeting specific files and folders, File Eraser enables you to ensure that log files are securely and completely erased at the end of their retention period.

Why Blancco?

Financial services industries are progressively relying on technological innovations to deliver services and conduct business quickly and efficiently. With that comes the increased need for robust data security and meticulous approaches to data protection.

For over 20 years, Blancco has offered solutions that support compliance with data protection and privacy regulations such as those put forth by Bangko Sentral ng Pilipinas. Our data erasure solutions have been tested, certified, approved and recommended by 15+ governing bodies and leading organizations around the world, providing solid assurance of complete and secure data erasure according to the desired requirements. We support the need for heavily regulated industries to stay compliant with these regulations and provide data erasure solutions that satisfy (and often exceed) their requirements.

Contact us today for information on how we can help you comply with the Philippine's Circular 982 for BSFIs by protecting financial, personal and private business data at the appropriate points within the data lifecycle across all IT data storage assets.

Learn more about Blancco's Data Erasure Solutions for Enterprise Organizations. Request a free trial today.