



BANGKO SENTRAL NG PILIPINAS

OFFICE OF THE DEPUTY GOVERNOR
SUPERVISION AND EXAMINATION SECTOR

MEMORANDUM NO. M-2014- 012

To : ALL BSP-SUPERVISED INSTITUTIONS

Subject : OBSOLESCENCE OF INFORMATION ASSETS

A. RISK MANAGEMENT PROCESSES TO ADDRESS OBSOLETE INFORMATION ASSETS

The product life cycle of an information asset generally ends when it is rendered obsolete, such as when the (1) skill required in maintaining the asset is no longer available, (2) supplier/vendor stops supporting the asset (end-of-life) or (3) format is no longer readable by more current technologies. Obsolescence heightens operational risk due to its implications to service delivery, information security and business continuity. For instance, end-of-life increases the vulnerability to malware and other attacks since the supplier/vendor no longer monitors and provides patches/security updates to the said asset.

In line with this, BSP supervised institutions (BSIs) should follow existing Information Technology (IT) risk management processes provided by BSP Circular No. 808 dated 22 August 2013 (including the related appendices), to address the risks brought about by obsolescence. Given that obsolescence is (1) an identified threat or (2) an event that may result to vulnerabilities to the information assets or over-all IT operations, such should be included in the risk assessments with corresponding risk management response and implementation plan, as applicable. In particular, the following provisions should be observed:

1. **"2. Risk Identification and Assessment.** xxx *An effective IT assessment process begins with the identification of the current and prospective IT risk exposures arising from the institution's IT environment and related processes. The assessments should identify all information assets, any foreseeable internal and external threats to these assets, the likelihood of the threats, and the adequacy of existing controls to mitigate the identified risks. xxx The probability of occurrence and the magnitude of impact provide the foundation for reducing risk exposures or establishing mitigating controls for safe, sound, and efficient IT operations appropriate to the complexity of the organization."*
2. **"3. IT Controls Implementation.** xxx *Management should establish an adequate and effective system of internal controls based on the degree of exposure and the potential risk of loss arising from the use of IT."*

Should the BSI opt to maintain the asset, supplementary controls may need to be considered, such as additional monitoring, isolation from the network or other protection from threat sources.

3. **Appendix 75b – “3.3.3 Ongoing risk assessment.** *The BSI should continuously gather and analyze information regarding new threats and vulnerabilities, actual attacks on the institution or others, and the effectiveness of the existing security controls. It should evaluate the information gathered to determine the extent of any required adjustments to the various components of the IS program. xxx”*

In addition, the BSP shall separately issue supplemental guidelines on software use, installation and retirement for Appendix 75c of Circular No. 808 to provide guidance on the management of lifecycle of software and other information assets.

B. END-OF-SUPPORT FOR WINDOWS XP

Windows XP, which was released in 2001, is widely used in the banking industry as the operating software (OS) for personal computers (PCs), servers and Automated Teller Machines (ATMs). As of March 2014, Windows XP dominates the ATM market powering more than 95%¹ of the world's machines. Meanwhile, though not specific to the banking industry, its share for PCs in the Philippines remains at around 20%² as of January 2014.

However, on 08 April 2014, technical assistance and automatic updates for Windows XP will no longer be available after more than 12 years of support. Microsoft claimed that as a result of the termination of support for Windows XP, security risk will be heightened since the lack of critical security updates makes PCs and other devices more vulnerable to harmful viruses, spyware and other malicious software which can steal or damage business data and information. Continued use may also lead to downtime and software issues, which may translate to customer dissatisfaction, delays in availing financial services, denial of service for customers and, in the worst case, financial losses. In addition, Windows XP's end-of-life may also have implications on the compliance status of BSIs that are subject to the requirements of Payment Card Industry Data Security Standard (PCI DSS) or other similar standards, since use of an outdated OS is not aligned with global security standards unless appropriate risk mitigation measures are in place.

Given that the end-of-life announcement for Windows XP was made as early as 2012, BSIs are expected to have already developed and implemented a plan to upgrade their operating system. Nevertheless, all BSIs that are affected should submit to the Core IT Specialist Group of the BSP an implementation and

¹ <http://www.businessweek.com/articles/2014-01-16/atms-face-deadline-to-upgrade-from-windows-xp>

² Based on Statcounter data

transition plan, signed by the President and Compliance Officer, within 20 calendar days from date of issuance of this memorandum.

For information and guidance.


NESTOR A. ESPENILLA, JR.
Deputy Governor

19 March 2014