



JOINT STATEMENT

END OF MICROSOFT SUPPORT FOR WINDOWS XP OPERATING SYSTEM

PURPOSE

The Federal Financial Institutions Examination Council (FFIEC) agencies¹ (“agencies”) are jointly issuing this statement to alert financial institutions that the discontinuation of support for the Microsoft Windows XP operating system (XP) could present operational risks to financial institutions, technology service providers (TSPs), and to activities supported by other third parties. The agencies expect financial institutions and TSPs to identify, assess, and manage these risks to ensure that safety, soundness, and the ability to deliver products and services are not compromised.

BACKGROUND

Microsoft will discontinue extended support for XP effective April 8, 2014. After this date, Microsoft will no longer provide regular security patches, technical assistance, or support for XP. Financial institutions, TSPs, and other third parties that use XP in personal computers, servers, and purpose-built devices such as automated teller machines (ATM), or that are dependent on applications that require use of XP could be exposed to increased operational risk.

POTENTIAL PROBLEMS

Potential problems include degradation in the delivery of various products and services, application incompatibilities, and increased potential for data theft and unauthorized additions, deletions, and changes of data. Additionally, financial institutions and TSPs that are subject to the requirements of the Payment Card Industry Data Security Standard (PCI DSS) and continue to use XP after April 8, 2014, may no longer be compliant.

REGULATORY GUIDANCE

Financial institutions and TSPs that use XP should follow their risk management processes to address the risk from the continued use of XP, consistent with the risk management

¹ Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, Consumer Financial Protection Bureau, State Liaison Committee.

guidance contained in the *FFIEC Information Technology (IT) Examination Handbook*. Important considerations include

- ***performing risk assessments:*** Identify and measure the risk from the continued use of XP throughout the organization and at third parties, including business continuity and disaster recovery situations.
- ***selecting appropriate mitigations:*** Consider costs and potential risks, including compatibility with other systems and applications, in selecting a mitigation strategy.²
- ***conducting appropriate planning:*** Develop an implementation plan addressing priorities for changes, ensuring appropriate change management procedures, and monitoring related third parties' mitigation and migration activities, as warranted.³
- ***monitoring and reporting:*** Monitor the risk mitigation implementation to ensure that the level of risk is acceptable. The effectiveness of controls should be tested periodically and results reported to senior management or a committee of the board of directors, as appropriate, to ensure risk continues to be managed.

² Broad mitigation options include replacing XP with a current operating system or maintaining XP over time. The latter option potentially includes implementing controls designed to provide additional monitoring for XP-supported systems and devices, protecting XP from threat sources, and isolating XP from the remainder of the network.

³ For further information and guidance, see the "Operations" booklet of the *FFIEC IT Examination Handbook* at <http://ithandbook.ffiec.gov/>.