

In October 2025, this attachment was revised to remove references to reputational risk.

Attachment A for SR letter 98-9

Revised October 2025

**Examples of Information Technology Elements that Should be Considered
in Assessing Business Risks of Particular Situations**

Situation	IT Elements to be Considered	Potential Effect on Business Risks	Risk Mitigants
A bank holding company expands very rapidly via acquisition into new product lines and geographic areas.	<p>Management Processes: Lack of clear, cohesive strategies could result in dependence on different systems that are incompatible and fragmented.</p> <p>Integrity: Unreliable information could be produced due to incompatible systems.</p> <p>Availability: Critical information may not be available to management when needed.</p>	<p>Credit Risk: Exposure may increase to less creditworthy borrowers.</p> <p>Liquidity Risk: Depositors may withdraw funds or close accounts due to unreliable account information.</p> <p>Operational Risk: Controls may be inadequate to address the increase in manual interventions to correct incompatibility problems between affiliates' systems, leading to a greater potential for fraudulent transactions.</p>	<ul style="list-style-type: none">• Develop a well thought-out plan for integrating acquired systems, mapping data-flows and sources, and ensuring reliability of systems.
A bank's consumer loan division inputs erroneous entries into the general ledger system.	<p>Integrity: Billing errors and unwarranted late payment fees could occur due to the inaccurate loan information maintained by the system.</p>	<p>Operational Risk: Increased expenditures may be required to resolve accounting operations problems.</p> <p>Legal Risk: Litigation could arise because of errors in customer accounts due to processing deficiencies.</p>	<ul style="list-style-type: none">• Improve policies and procedures related to input of accounting entries.• Ensure internal audit considers system aspects of accounting operations.

<p>Substantial turnover occurs in bank's wire transfer department.</p>	<p>Security: Security procedures could be compromised due to inadequate training and lack of qualified personnel.</p> <p>Integrity: System may not be able to provided "real time" funds availability.</p>	<p>Operational Risk: Financial losses could occur due to fraud or incorrectly sent wire transfers.</p> <p>Legal Risk: Litigation could arise as a result of errors in customer accounts and fraudulent wire transfers.</p>	<ul style="list-style-type: none"> • Increase and strengthen procedural and access controls for wire operations. • Implement security measures such as passwords and firewalls. • Develop and monitor appropriate audit trails. • Provide for adequate training program and staffing levels.
--	--	--	--