

The Five Biggest Mistakes Banks Make in Managing Risk

Jim Bolyard, CISA, CISM, CGEIT, Senior IT Audit Officer – DCI (Data Center Inc.)

Every month, a hot new technology promises to be – and in some cases truly is – the next big thing in banking. As community banks implement new technology systems that may be vital to growth and marketplace competition, many of them are left open to unnecessary and potentially devastating risks that are easily avoided with a little planning.

Here is a look at five of the biggest mistakes community banks make when evaluating new technologies and the potential risk involved.

1. Failure to establish a risk plan

Risk and uncertainty is inherent to any size organization, and every new technology carries a level of risk. Bank personnel must establish a risk plan, while researching the technology and before implementation. A proper plan includes identifying potential risks, determinants of the risks, and effective solutions that counter each potential issue.

Risk can be divided into two parts: protecting against any financial loss related to products or services, or ensuring financial income creation opportunities are not missed or lost. Understanding and managing risk is key for creating an adequate risk identification and mitigation process, safeguarding all financial assets. Financial organization staff should understand all their potential business risks.

Effective risk analysis begins by understanding the nature of risks faced by the institution and how they interrelate.

However, don't forget about the residual risk – the amount of financial loss institutions are willing to sustain before spending additional money on IT related risks.

Some potential areas to establish and maintain an all-encompassing risk management process are:

1. Identify and document the risk ownership of the ongoing process
2. Hire a Chief Information Security Officer
3. Leverage your organization "brain trust", i.e. IT security, operations, Chief Information Officer, Legal counsel, Business unit managers, physical security, Internal/IT audit, Chief Risk Officer

2. Failure to include all managers and departments involved

A risk management plan should not be designated to just one “fix-it” person at the bank. All departments and managers should have input, as the technology or system may affect all areas of the bank – from operations to human resources and compliance.

Risk reporting must be driven by a “tone from the top” approach, which provides a continuous process of risk identification, monitoring, feedback and maintaining appropriate availability and accessibility.

Obtaining input and buy-in from each department increases a technology’s chance of success when all parties are educated on the system. Further, by integrating the management of IT risk into the overall enterprise risk management of the organization, your management can make better decisions about potential risk, as well as the risk appetite and tolerance of the institution, and how to respond to the risk.

3. Failure to achieve board buy-in

Ultimately, the board is responsible for everything that occurs at the bank – success and failure alike. When presenting new technologies to the board, ease their concerns and gain buy-in by including a risk analysis and management plan. Collective support of a technology initiative from top to bottom greatly increases the potential for success.

4. Failure to keep the risk plan updated

Remember that the risk management process is a living process and should become part of the institutions daily processes and continue to be updated and enhanced. An outdated, nonfunctioning plan is as useless as a nonexistent plan. The bank’s risk management plan should be updated at least one a year in addition to regular testing to verify that all components of the plan are viable. Also remember, establishing a complete reporting structure for your institution’s risk management process from the Board of Directors level down to the institution’s staff, is very critical to the functionality of the process.

Take action to enhance your risk management process tailored to your institution.

1. Improve your IT controls and procedures
2. Prioritize and manage the business risks – loss of confidentiality, integrity and availability

3. Frequently monitor, assess and report the process throughout the institution's Senior Management, Audit Committees and Board of Directors.
4. Automate the collection / identification of IT processes and controls
5. Establish financial risk objectives and measure the results

5. Failure to ask for outside assistance

A bank's core processor and other vendor partners have vital technical expertise and often work with banks of different asset sizes, localities and business models. Their experience can provide broader insight and guidance to individual banks for a new technology risk assessment.

Community banks must understand that while risk is inevitable, the impact is greater for them than their larger counterparts. Whether these risks are researched and planned for with proper procedures will ultimately determine the success or failure of new systems and programs. Banks that are mindful of new technology hurdles are more likely to integrate new systems seamlessly and to quickly reap and pass along their benefits.

—Jim Bolyard, CISA, CISM, CGEIT, is the Senior IT Audit Officer at Hutchinson, Kansas-based DCI (www.datacenterinc.com), a provider of full-service core bank technology and processing solutions to the financial industry. Mr. Bolyard has over 20 years of banking and audit experience, has taught at the college-level on banking and auditing. He is a Certified Information Systems Auditor, Certified Information Security Manager, Certified in the Governance of Enterprise IT, and also currently serves as the President of the Wichita, Kan. chapter of the Institute of Internal Auditors.

Largest Business Risks Involving IT

source: Information Systems Auditing and Control Association

