

The Impact of Customer Information Technology on the Lending Decision

JOEL LANZ, JAMES J. ARMETTA, AND JENNIFER KIELY

JOEL LANZ is a partner in Andersen's metro New York technology risk consulting practice.

JAMES J. ARMETTA is a senior manager in Andersen's metro New York technology risk consulting practice.

JENNIFER KIELY is a consultant in Andersen's metro New York technology risk consulting practice.

The ability to measure, manage, monitor, and mitigate risks comprehensively requires skills that go far beyond the historical credit reviews and relationship instincts of the past. As borrowers increase their reliance on information technology (IT), lenders must be able to conduct due diligence on a prospective borrower's technological and operational safety and soundness.

IT is a significant enabler of business through many and varied applications: eBusiness, customer relationship management, supply chain management, electronic procurement, and enhanced automated manufacturing and service delivery functions, for example. Many companies' sales and success are directly affected by their ability to manage IT effectively.

Today's lenders rely extensively on complex credit-risk models to assess, control, and reduce risk and to ensure that their portfolios are in line with their overall corporate strategies. Lenders have modified their credit-risk-management strategies to keep pace with competitive market conditions, narrow spreads, and complexity.

In addition, lenders must strive to understand the impact that IT can have on a customer's business and to evaluate the risk (possibly formidable) of technology problems in making lending decisions. This article will familiarize lenders with the key issues to consider when assessing a credit that depends on IT to achieve critical business goals.

THE IMPACT OF TECHNOLOGY ON THE LENDING DECISION

Perhaps the impact of IT can be best illustrated by considering a specialty finance company that has significant lines of credit from various lenders. IT pervades all aspects of the specialty finance company's business, from the initiation of a receivable transaction through funding to financial reporting and, of course, the underlying back-office processing. Exhibit 1 illustrates critical examples of the areas and functions affected by IT.

So why should a lender be concerned with the technology its borrowers are using? Four reasons: It affects the integrity of financial information used in the credit decision. It significantly affects the operations of the business. In many businesses, IT is the single largest expense item. Failure to manage or implement new technology could endanger a customer's competitive position. All four could severely affect the customer's ability to maintain required loan covenants or repay the loan.

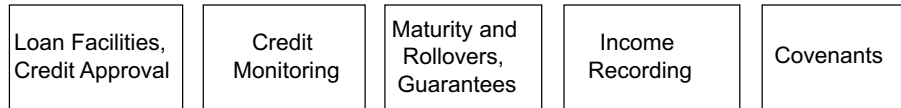
WHAT MUST CREDITORS KNOW?

Credit professionals do not need to understand the intricacies of combining a client-server distributed system with a mainframe environment that links to the Web via an n-tier architecture. However, they need to appreciate their customer's ability to manage IT effectively and efficiently so that desired

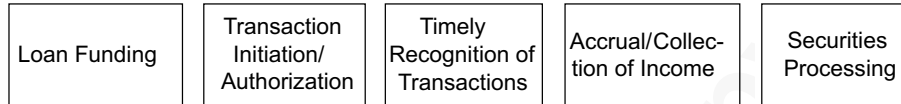
EXHIBIT 1

IT Affects All Aspects of Many Businesses—Example: Specialty Finance Company

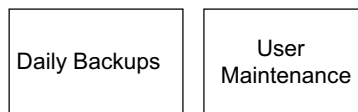
Credit and Structured Finance



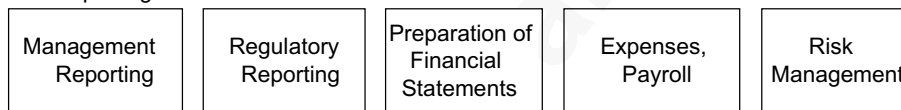
Treasury and Investment Processing



IT and Back-Office



Financial Reporting



results can be achieved. By considering the following five IT risk-management questions, lenders should begin to obtain a sufficient appreciation of their customer's ability to effectively support business goals by properly managing IT:

- Do any concerns exist with the risks associated with the integrity of system information or the authorization, completeness, and accuracy of transactions as they are entered into, processed by, summarized by, and reported on by the various application systems deployed by the firm (integrity)?
- Is the continuity of the firm's critical operations and processes threatened from unavailability of important processing and information when needed (availability)?
- Is access to information (data or programs) adequately restricted to prevent unauthorized knowledge and use or disclosure of confidential information or is access to information overly restrictive, thereby keeping personnel from performing their assigned responsibilities effectively and efficiently (access)?

- Does the firm have the information technology infrastructure (for example, hardware, networks, software, people, and processes) it needs to effectively support the current and future information requirements of the business in an efficient, cost-effective, and well-controlled fashion (infrastructure)?
- Do the systems produce the relevant information needed by management to effectively manage the business and support critical decisions (relevance)?

Lenders need to appreciate their customer's ability to manage IT effectively and efficiently so that desired results can be achieved.

The issues that lenders should consider when answering these five questions or areas—integrity, availability, access, infrastructure, and relevance—are discussed below.

INTEGRITY

This consideration encompasses all of the risks associated with the authorization, completeness, and accuracy of transactions as they are entered into, processed by, summarized by, and reported on by the various application systems deployed by a business. These risks apply pervasively to each and every aspect of an application system used to support a business process and are present in multiple places and at multiple times throughout application systems. However, they principally manifest themselves in the following components of an application system:

- user interface,
- processing,
- error processing,
- interface,
- change management,
- data.

Integrity can be lost because of programming errors (for example, good data is processed by incorrect programs); processing errors (for example, transactions are incorrectly processed more than once against the same master file); or management processing errors (for example, poor management of the system's maintenance process).

To consider whether customer management is taking the necessary steps to ensure the integrity of the information and related processing of the business, lenders should ask the following six questions:

- ***Does the customer have a comprehensive data management plan that defines goals and policies for the collection, structure, and management of data assets?*** This is important because it lays the foundation for responsibility over data assets. The lack of formal planning and administration can mean that database integrity is at risk because routine operations and maintenance are not consistent. Also, data repositories may not be configured and maintained based on changing business needs or performance requirements—resulting in processing bottlenecks and inaccurate data on which to perform business activities.
- ***Do the customer's users and managers lack confidence in the availability, integrity, or relevance of data? Have service levels for database response time, availability, and restoration of lost or corrupt data been established? Are they being met?*** User dissatisfaction is often a key symptom of poor IT management.

Lack of planning and formal agreements lead to the risk that data cannot be retrieved in a timely manner to support either existing key processes or anticipated new processes. This can potentially result in the loss of customers and business partners. In addition, if priorities are not adequately defined, the relationship between IT and the business users may deteriorate because users view IT as unresponsive and IT views users as imposing frequent burdensome design changes. The bottom line: IT investments are not being effectively leveraged to support the business goals that justified the investment in the first place.

- ***Are the processes to collect, process, and distribute data and information duplicated or inefficient?*** If yes, the customer may incur unnecessary expenditures and receive delayed service because processes are not in place to collect, store, and manage data in an effective and efficient manner.
- ***Is frequent manual intervention required to keep databases operational?*** Frequent logical or physical database reorganization can be costly. It also means that database performance management depends on human intervention that is subject to error. This may adversely impact enterprisewide performance and the availability of the systems that support the underlying business processes.
- ***Has data ever been lost or unrecoverable due to the absence of backup, restore, or recovery procedures?*** If a business maintains its assets electronically (for example, a leasing company), the inability to recover the resources maintaining those assets could lead to significant disruptions in the business—including the failure of the business. In addition, such downgrading of service may lead a customer's clientele to move to a competitor.
- ***Are tools and procedures available for synchronizing databases or to periodically validate data integrity?*** If not, customer service and decision making may be impaired because data critical to support key business processes may not exist, may be difficult to obtain, or may be inaccurate.

AVAILABILITY

Simply put, availability risk is the risk that information and system resources will not be available when needed. It includes risks such as loss of communications (for example, cut cables, telephone system outage, satel-

EXHIBIT 2

A Checklist of Technology Risks

Risk Area	Risk Indicators	Mitigated	Not mitigated	N/A	Comments
Integrity	<ul style="list-style-type: none"> No comprehensive data management plan that defines goals and policies for the collection, structure, and management of data assets. Users and managers lack confidence in the availability, integrity, or relevancy of data. Duplication of processes to collect, process, and distribute data and information. Frequent and costly logical or physical database reorganization needed to support new business processes. Service levels for database response time, availability, and restoration of lost or corrupt data have not been established and/or are not being met. Data has been lost or is unrecoverable due to the absence of back-up, restore, or recovery procedures. Tools and procedures are not available for synchronizing databases or to periodically validate data integrity. Frequent manual intervention is required for keeping databases operational. 				
Availability	<ul style="list-style-type: none"> No documented enterprisewide business continuity plan. No assignment of accountability and responsibility for managing the business continuity process or its specific tasks. No process to conduct a business impact analysis to identify and rank critical business functions, their associated applications, databases, and related resources needs. No process to perform threat/vulnerability analysis to identify the source and likelihood of occurrence of specific threats in order to plan recovery actions as well as risk mitigation steps. No process to regularly test and, as needed, update continuity plans. Failure to consider both technology and nontechnology requirements to recover and sustain business functions. Absence of service-level agreements defining acceptable outage time frames based on the business function's criticality and internal/external requirements (that is, business units, vendor/customer contracts, legal/regulatory requirements, etc.). No process to develop and deploy strategies for the use of alternative resources and facilities to conduct business after an outage occurs. 				
Access	<ul style="list-style-type: none"> No formal security vision, directives, or policy endorsed by the client's senior or executive management regarding the protection of data assets. No formal security standards or procedures. Responsibility and accountability for securing data assets has not been assigned. Frequent unauthorized access to data or IT resources. No formal monitoring of security logs to identify and address potential intrusions or inappropriate use of data assets. Inability to control access on a "need-to-have" basis in order to perform job duties. Absence of audit trails to track changes to security configuration and options or parameters. 				
Infrastructure	<ul style="list-style-type: none"> Large number of infrastructure management tools deployed in the environment that do not appear to be managed centrally. A framework product is not effectively deployed or multiple framework products are deployed. The organization is not able to provide documentation about critical business process flows. Infrastructure management SLAs have not been defined or are poorly defined. 				
Relevance	<ul style="list-style-type: none"> Competitive gap widening between organization and its competitor. Increased backlog of business applications. Dissatisfaction with formal IT organization. High turnover in executive leadership: CIOs, CTOs, and others. Increased use of consultants or outsourcers for strategic versus specific tasks. Mergers, acquisitions, or other major business changes stressing capabilities of IT. Attrition of IT skills. Increasing IT budget overruns. 				

lite loss); loss of basic processing capability (for example, fire, flood, electrical outage); and operational difficulties (for example, disk drive breakdown, operator errors). Business interruption can also arise from natural disasters, vandalism, sabotage, and accidents. The company's ability to continue critical operations and processes may be highly dependent on availability of certain information systems. If critical or important systems go down for an unacceptable period, a company can experience difficulty in continuing operations. Why should a lender be concerned? Critical and important information systems that are not available to sustain operations can result in loss of revenue, cash flow, and profits; loss of competitive advantage; dissatisfied customers and loss of market share; increased costs; loss of employee morale; and, depending on the industry, fines and sanctions.

Availability risk focuses on three different levels of risk:

- risks that can be avoided by monitoring performance and proactively addressing systems issues before a problem occurs;
- risks associated with short-term disruptions to systems where restore/recovery techniques can be used to minimize the extent of a disruption;
- risks associated with disasters that cause longer-term disruptions in information processing and that focus on controls such as backups and contingency planning.

To address the area of availability, the lender should ask the following five questions:

Does the business have a documented enterprise-wide business continuity plan? Is responsibility for managing the business continuity process assigned to a specific team or person? A business continuity plan enables the business to recover and continue serving its customers. In some industries, this type of plan is a regulatory requirement. Failure to adequately plan for a disruption can harm revenues, because customers may go elsewhere to obtain the services they desire.

Do service-level agreements (SLA) exist that define acceptable outage time frames? Have strategies been established for the use of alternative resources and facilities to conduct business after an outage occurs? SLAs should be based on the business function's criticality and internal/external requirements (that is, business units, vendor/customer contracts, legal/regulatory requirements, etc.). This becomes especially important if the customer

outsources its system-processing activities to a third party. If need be, incentives should be incorporated to encourage third-party servicer compliance with the SLA. As required, alternative plans and strategies should be available in the case that poor performance jeopardizes business operations.

Has the organization conducted a business impact analysis to identify and rank critical business functions, their associated applications, databases, and related resources needs? All well-managed organizations should have a process to perform a threat/vulnerability analysis to identify the source and likelihood of occurrence of specific threats in order to plan recovery actions as well as risk mitigation steps. If not, your borrower may suffer from inability or delays in recovering critical business processes necessary to sustain business operations.

Is there a process to regularly test and update continuity plans? Business continuity plans are not static. They must mirror changes in the business. If the plan has not been regularly reviewed, the organization may have a false sense of security due to dated or untested processes.

Have both technology and nontechnology requirements been considered to recover and sustain business functions? If all aspects of the organization are not considered, the company may be unable to deploy sufficient human, technical, or physical resources to the appropriate locations to activate and execute the continuity plan. This can lead to loss of competitive market position and public image. Ultimately, failure to reestablish an acceptable level of operations can cause the business to cease to exist. We have seen numerous situations where a disaster recovery plan existed for the data center, but because the plan did not consider the user perspective, the business was not able to recover appropriately.

ACCESS

Access risk is the risk that access to information (data or programs) will be inappropriately granted or refused. Inappropriate people may be able to access confidential information. Appropriate personnel may be denied access. Access risk focuses on the risks associated with inappropriate access to systems, data, or information. It encompasses the risks of improper segregation of duties, risks associated with the integrity of data and databases, and risks associated with information confidentiality, etc. Access risk can occur at any, or all, of the following five levels:

- network,
- processing environment,
- application system,
- functional access (within an application),
- field-level access (within a function).

Lenders should consider the following five questions as they evaluate their customers' risk:

Has a formal security vision, directive, or policy been endorsed by the customer's senior or executive management regarding the protection of data assets? Failure of executive management to impose a control framework can have any number of ramifications up to and including legal exposure and fines due to violations of legal and regulatory requirements to protect data assets.

Have formal security standards or procedures been established? Has responsibility and accountability for securing data assets been assigned? Failure to establish proper standards and procedures increases the risk of unauthorized modification, destruction, or disclosure of data resulting in costly business process interruptions and potential loss of assets maintained electronically.

Does unauthorized access to data or IT resources occur? Are audit trails used to track changes to security configuration and options or parameters? Accidental or deliberate violations of access can lead to unnecessary expenditures to recover or replace damaged or deleted files.

Does formal monitoring of security logs take place to identify and address potential intrusions or inappropriate use of data assets? While prevention is the best cure, organizations should also monitor security. Failure to do so can result in misuse of confidential information. This can cause IT to lose the trust and respect of internal users, customers, suppliers, and vendors.

Has access been restricted to a need-to-have basis in order to perform job duties? The system should enforce organizational controls that help promote segregation of duties and reduce the opportunity for incorrect or unauthorized processing.

INFRASTRUCTURE

Infrastructure risk is the risk that the firm does not have an effective information technology infrastructure (for example, hardware, networks, software, people, and processes) to effectively support the current and future needs of the business in an efficient, cost-effective, and well-controlled fashion. These risks relate to the processes used to define, develop, maintain, and operate an information-pro-

cessing environment (for example, computer hardware, networks) and the associated application systems (for example, customer service, accounts payable).

The risks are generally considered within the context of the following core IT processes:

- organizational planning,
- application system definition and deployment,
- logical security and security administration,
- computer and network operations,
- data and database management,
- business/data center recovery.

Lack of effective and well-controlled business processes in each of these areas are often the root cause of the access, relevance, and availability risks listed above.

Lenders should ask the following three questions about infrastructure management:

Is the organization able to provide documentation regarding critical business process flows? Inability to map key information flows may be an indication that an organization is having difficulty with its infrastructure or cannot maintain appropriate inventories of the assets invested in the infrastructure.

Have infrastructure management SLAs been defined? If not, the efficiency and effectiveness of important business processes that depend upon information and other technology performance will suffer and could adversely affect business performance.

To what extent are infrastructure management tools deployed in the IT environment? Are they managed from a central locale? Poor selection of tools leads to the risk that infrastructure management software costs may be excessive. As a result, many tools will either be "shelfware" (purchased and never used) or underused. At best, the business may achieve less than acceptable performance and lack competitive advantage. Worse still, the business may experience suboptimal financial returns on its IT investment and performance.

RELEVANCE

Relevance risk is the risk that information is not relevant to the purposes for which it is collected, maintained, or distributed. This risk relates to the usability and timeliness of information that is either created or summarized by an application system. Relevance risk is the risk associated with not getting the *right* data/information to the *right* person/process/system at the *right* time to allow the

right action to be taken. This risk arises frequently from a failure to fully understand information needs and a lack of attention to timeliness issues.

Lenders should ask five key questions in relation to this key issue:

Is the organization perceived as a technology leader in the market, or is there a perceived competitive gap widening between the organization and its competitors?

Failure to appropriately manage technology can lead to a perceived loss of competitive position in the market, increased internal and external customer dissatisfaction with service provided, and potential damage to an organization's long-term business reputation. Ultimately, this can result in lost revenue opportunities due to inability of IT to satisfy business objectives.

What is the level of user satisfaction with the IT organization? An increased backlog of business applications, for example, may indicate that the IT department is having problems in continuing to serve the evolving needs of the business.

Has there been a high turnover in executive leadership: chief information officer, chief technology officer, and others? Any recent attrition of IT skills? Has there been increased use of consultants or outsourcers for strategic vs. specific tasks? This could be an indication of the customer's ineffectiveness in properly leveraging technology to solve business challenges.

Have there been/are there any planned mergers, acquisitions, or other major business changes placing stress on the capabilities of IT? Increased pressures on the IT department may result in solutions that are compromised and fail to meet business requirements. Furthermore, the organization may be unable to launch new products and services on time.

What has been the pattern of IT spending? Increasing IT budget overruns may be an indicator of difficulties in managing technology. A corporate lender should be concerned if the organization is making excessive investments in IT with minimal return.

INCORPORATING TECHNOLOGY INTO THE LENDING DECISION

Where and how the types of questions shown above should be considered is up to the lending professional. Perhaps it can be covered in a due-diligence report by an advisor or credit audit specialist. Maybe it should be a discrete scoring item in a credit-risk model—or a result of a periodic relationship meeting with the customer. What it should not be is overlooked.

These are challenging times for lenders. The pessimistic economic environment is dampening enthusiasm for new projects and ventures, not to mention creating challenges with current outstanding credits. A further headache for the lender results from how the forecast explosion in information arising out of business-to-business e-commerce poses data mining, risk analysis, and new business opportunities for new, nimble entrants (and, thus, threats to established lenders). Amid all these risks, the last thing many lenders expect to have to consider is technology. But a company's technology is potentially its single greatest competitive asset, its greatest cost component—and its greatest risk. To ignore the technology issues that face a borrower is to ignore the backbone on which its business runs.