Inherent Risk Profile

Category: Technologies and Connection Types	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Total number of Internet service provider (ISP) connections (including branch connections)	No connections	Minimal complexity (1–20 connections)	Moderate complexity (21–100 connections)	Significant complexity (101–200 connections)	Substantial complexity (>200 connections)
Unsecured external connections, number of connections not users (e.g., file transfer protocol (FTP), Telnet, rlogin)	None	Few instances of unsecured connections (1–5)	Several instances of unsecured connections (6–10)	Significant instances of unsecured connections (11–25)	Substantial instances of unsecured connections (>25)
Wireless network access	No wireless access	Separate access points for guest wireless and corporate wireless	Guest and corporate wireless network access are logically separated; limited number of users and access points (1–250 users; 1–25 access points)	Wireless corporate network access; significant number of users and access points (251–1,000 users; 26–100 access points)	Wireless corporate network access; all employees have access; substantial number of access points (>1,000 users; >100 access points)
Personal devices allowed to connect to the corporate network	None	Only one device type available; available to <5% of employees (staff, executives, managers); e-mail access only	Multiple device types used; available to <10% of employees (staff, executives, managers) and board; e-mail access only	Multiple device types used; available to <25% of authorized employees (staff, executives, managers) and board; e-mail and some applications accessed	Any device type used; available to >25% of employees (staff, executives, managers) and board; all applications accessed
Third parties, including number of organizations and number of individuals from vendors and subcontractors, with access to internal systems (e.g., virtual private network, modem, intranet, direct connection)	No third parties and no individuals from third parties with access to systems	Limited number of third parties (1–5) and limited number of individuals from third parties (<50) with access; low complexity in how they access systems	Moderate number of third parties (6–10) and moderate number of individuals from third parties (50–500) with access; some complexity in how they access systems	Significant number of third parties (11–25) and significant number of individuals from third parties (501–1,500) with access; high level of complexity in terms of how they access systems	Substantial number of third parties (>25) and substantial number of individuals from third parties (>1,500) with access; high complexity in how they access systems

Category: Technologies and Connection Types	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Wholesale customers with dedicated connections	None	Few dedicated connections (between 1–5)	Several dedicated connections (between 6–10)	Significant number of dedicated connections (between 11–25)	Substantial number of dedicated connections (>25)
Internally hosted and developed or modified vendor applications supporting critical activities	No applications	Few applications (between 1–5)	Several applications (between 6–10)	Significant number of applications (between 11–25)	Substantial number of applications and complexity (>25)
Internally hosted, vendor-developed applications supporting critical activities	Limited applications (0–5)	Few applications (6–30)	Several applications (31–75)	Significant number of applications (76–200)	Substantial number of applications and complexity (>200)
User-developed technologies and user computing that support critical activities (includes Microsoft Excel spreadsheets and Access databases or other user-developed tools)	No user-developed technologies	1–100 technologies	101–500 technologies	501–2,500 technologies	>2,500 technologies
End-of-life (EOL) systems	No systems (hardware or software) that are past EOL or at risk of nearing EOL within 2 years	Few systems that are at risk of EOL and none that support critical operations	Several systems that will reach EOL within 2 years and some that support critical operations	A large number of systems that support critical operations at EOL or are at risk of reaching EOL in 2 years	Majority of critical operations dependent on systems that have reached EOL or will reach EOL within the next 2 years or an unknown number of systems that have reached EOL
Open Source Software (OSS)	No OSS	Limited OSS and none that support critical operations	Several OSS that support critical operations	Large number of OSS that support critical operations	Majority of operations dependent on OSS
Network devices (e.g., servers, routers, and firewalls; include physical and virtual)	Limited or no network devices (<250)	Few devices (250–1,500)	Several devices (1,501–25,000)	Significant number of devices (25,001–50,000)	Substantial number of devices (>50,000)
Third-party service providers storing and/or processing information that support critical activities (Do not have access to internal systems, but the institution relies on their services)	No third parties that support critical activities	1–25 third parties that support critical activities	26–100 third parties that support critical activities	101–200 third parties that support critical activities; 1 or more are foreign-based	>200 third parties that support critical activities; 1 or more are foreign-based

Category: Technologies and Connection Types	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Cloud computing services hosted externally to support critical activities	No cloud providers	Few cloud providers; private cloud only (1–3)	Several cloud providers (4–7)	Significant number of cloud providers (8–10); cloud-provider locations used include international; use of public cloud	Substantial number of cloud providers (>10); cloud-provider locations used include international; use of public cloud

Category: Delivery Channels	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Online presence (customer)	No Web-facing applications or social media presence	Serves as an informational Web site or social media page (e.g., provides branch and ATM locations and marketing materials)	Serves as a delivery channel for retail online banking; may communicate to customers through social media	Serves as a delivery channel for wholesale customers; may include retail account origination	Internet applications serve as a channel to wholesale customers to manage large value assets
Mobile presence	None	SMS text alerts or notices only; browser-based access	Mobile banking application for retail customers (e.g., bill payment, mobile check capture, internal transfers only)	Mobile banking application includes external transfers (e.g., for corporate clients, recurring external transactions)	Full functionality, including originating new transactions (e.g., ACH, wire)
Automated Teller Machines (ATM) (Operation)	No ATM services	ATM services offered but no owned machines	ATM services managed by a third party; ATMs at local and regional branches; cash reload services outsourced	ATM services managed internally; ATMs at U.S. branches and retail locations; cash reload services outsourced	ATM services managed internally; ATM services provided to other financial institutions; ATMs at domestic and international branches and retail locations; cash reload services managed internally

Category: Online/Mobile Products and Technology Services	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Issue debit or credit cards	Do not issue debit or credit cards	Issue debit and/or credit cards through a third party; <10,000 cards outstanding	Issue debit or credit cards through a third party; between 10,000–50,000 cards outstanding	Issue debit or credit cards directly; between 50,000–100,000 cards outstanding	Issue debit or credit cards directly; >100,000 cards outstanding; issue cards on behalf of other financial institutions
Prepaid cards	Do not issue prepaid cards	Issue prepaid cards through a third party; <5,000 cards outstanding	Issue prepaid cards through a third party; 5,000–10,000 cards outstanding	Issue prepaid cards through a third party; 10,001–20,000 cards outstanding	Issue prepaid cards internally, through a third party, or on behalf of other financial institutions; >20,000 cards outstanding
Emerging payments technologies (e.g., digital wallets, mobile wallets)	Do not accept or use emerging payments technologies	Indirect acceptance or use of emerging payments technologies (customer use may affect deposit or credit account)	Direct acceptance or use of emerging payments technologies; partner or co-brand with non-bank providers; limited transaction volume	Direct acceptance or use of emerging payments technologies; small transaction volume; no foreign payments	Direct acceptance of emerging payments technologies; moderate transaction volume and/or foreign payments
Person-to-person payments (P2P)	Not offered	Customers allowed to originate payments; used by <1,000 customers or monthly transaction volume is <50,000	Customers allowed to originate payments; used by 1,000–5,000 customers or monthly transaction volume is between 50,000–100,000	Customers allowed to originate payments; used by 5,001–10,000 customers or monthly transaction volume is between 100,001–1 million	Customers allowed to request payment or to originate payment; used by >10,000 customers or monthly transaction volume >1 million
Originating ACH payments	No ACH origination	Originate ACH credits; daily volume <3% of total assets	Originate ACH debits and credits; daily volume is 3%–5% of total assets	Sponsor third-party payment processor; originate ACH debits and credits with daily volume 6%–25% of total assets	Sponsor nested third-party payment processors; originate debits and credits with daily volume that is >25% of total assets
Originating wholesale payments (e.g., CHIPS)	Do not originate wholesale payments	Daily originated wholesale payment volume <3% of total assets	Daily originated wholesale payment volume 3%–5% of total assets	Daily originated wholesale payment volume 6%–25% of total assets	Daily originated wholesale payment volume >25% of total assets

Category: Online/Mobile Products and Technology Services	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Wire transfers	Not offered	In person wire requests only; domestic wires only; daily wire volume <3% of total assets	In person, phone, and fax wire requests; domestic daily wire volume 3%–5% of total assets; international daily wire volume <3% of total assets	Multiple request channels (e.g., online, text, e-mail, fax, and phone); daily domestic wire volume 6%–25% of total assets; daily international wire volume 3%–10% of total assets	Multiple request channels (e.g., online, text, e-mail, fax, and phone); daily domestic wire volume >25% of total assets; daily international wire volume >10% of total assets
Merchant remote deposit capture (RDC)	Do not offer Merchant RDC	<100 merchant clients; daily volume of transactions is <3% of total assets	100–500 merchant clients; daily volume of transactions is 3%–5% of total assets	501–1,000 merchant clients; daily volume of transactions is 6%–25% of total assets	>1,000 merchant clients; daily volume of transactions is >25% of total assets
Global remittances	Do not offer global remittances	Gross daily transaction volume is <3% of total assets	Gross daily transaction volume is 3%–5% of total assets	Gross daily transaction volume is 6%–25% of total assets	Gross daily transaction volume is >25% of total assets
Treasury services and clients	No treasury management services are offered	Limited services offered; number of clients is <1,000	Services offered include lockbox, ACH origination, and remote deposit capture; number of clients is between 1,000–10,000	Services offered include accounts receivable solutions and liquidity management; number of clients is between 10,001–20,000	Multiple services offered including currency services, online investing, and investment sweep accounts; number of clients is >20,000
Trust services	Trust services are not offered	Trust services are offered through a third-party provider; assets under management total <$500 million	Trust services provided directly; portfolio of assets under management total $500 million–$999 million	Trust services provided directly; assets under management total $1 billion–$10 billion	Trust services provided directly; assets under management total >$10 billion
Act as a correspondent bank (Interbank transfers)	Do not act as a correspondent bank	Act as a correspondent bank for <100 institutions	Act as a correspondent bank for 100–250 institutions	Act as a correspondent bank for 251–500 institutions	Act as a correspondent bank for >500 institutions

Category: Online/Mobile Products and Technology Services	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Merchant acquirer (sponsor merchants or card processor activity into the payment system)	Do not act as a merchant acquirer	Act as a merchant acquirer; <1,000 merchants	Act as a merchant acquirer; outsource card payment processing; 1,000–10,000 merchants	Act as a merchant acquirer and card payment processor; 10,001–100,000 merchants	Act as a merchant acquirer and card payment processor; >100,000 merchants
Host IT services for other organizations (either through joint systems or administrative support)	Do not provide IT services for other organizations	Host or provide IT services for affiliated organizations	Host or provide IT services for up to 25 unaffiliated organizations	Host or provide IT services for 26–50 unaffiliated organizations	Host or provide IT services for >50 unaffiliated organizations

Category: Organizational Characteristics	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Mergers and acquisitions (including divestitures and joint ventures)	None planned	Open to initiating discussions or actively seeking a merger or acquisition	In discussions with at least 1 party	A sale or acquisition has been publicly announced within the past year, in negotiations with 1 or more parties	Multiple ongoing integrations of acquisitions are in process
Direct employees (including information technology and cybersecurity contractors)	Number of employees totals <50	Number of employees totals 50–2,000	Number of employees totals 2,001–10,000	Number of employees totals 10,001–50,000	Number of employees is >50,000
Changes in IT and information security staffing	Key positions filled; low or no turnover of personnel	Staff vacancies exist for non-critical roles	Some turnover in key or senior positions	Frequent turnover in key staff or senior positions	Vacancies in senior or key positions for long periods; high level of employee turnover in IT or information security
Privileged access (Administrators–network, database, applications, systems, etc.)	Limited number of administrators; limited or no external administrators	Level of turnover in administrators does not affect operations or activities; may utilize some external administrators	Level of turnover in administrators affects operations; number of administrators for individual systems or applications exceeds what is necessary	High reliance on external administrators; number of administrators is not sufficient to support level or pace of change	High employee turnover in network administrators; many or most administrators are external (contractors or vendors); experience in network administration is limited

Category: Organizational Characteristics	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Changes in IT environment (e.g., network, infrastructure, critical applications, technologies supporting new products or services)	Stable IT environment	Infrequent or minimal changes in the IT environment	Frequent adoption of new technologies	Volume of significant changes is high	Substantial change in outsourced provider(s) of critical IT services; large and complex changes to the environment occur frequently
Locations of branches/business presence	1 state	1 region	1 country	1–20 countries	>20 countries
Locations of operations/data centers	1 state	1 region	1 country	1–10 countries	>10 countries

Category: External Threats	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Attempted cyber attacks	No attempted attacks or reconnaissance	Few attempts monthly (<100); may have had generic phishing campaigns received by employees and customers	Several attempts monthly (100– 500); phishing campaigns targeting employees or customers at the institution or third parties supporting critical activities; may have experienced an attempted Distributed Denial of Service (DDoS) attack within the last year	Significant number of attempts monthly (501–100,000); spear phishing campaigns targeting high net worth customers and employees at the institution or third parties supporting critical activities; Institution specifically is named in threat reports; may have experienced multiple attempted DDoS attacks within the last year	Substantial number of attempts monthly (>100,000); persistent attempts to attack senior management and/or network administrators; frequently targeted for DDoS attacks

Total	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Number of Statements Selected in Each Risk Level					
Based on Individual Risk Levels Selected, Assign an Inherent Risk Profile	**Least**	**Minimal**	**Moderate**	**Significant**	**Most**