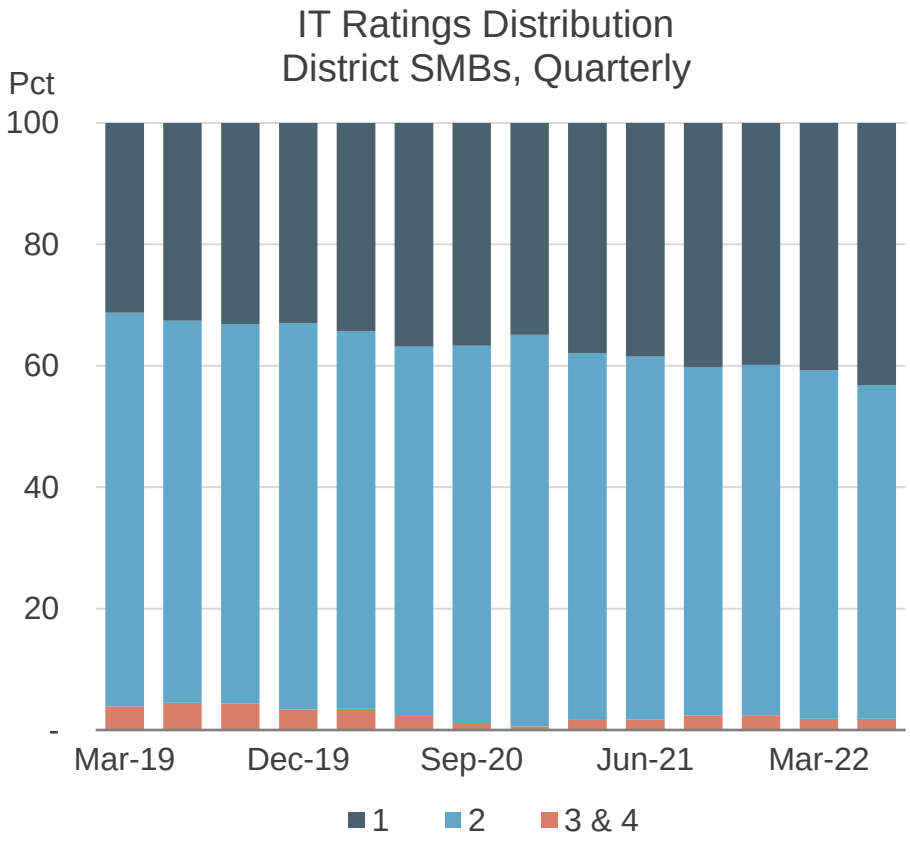
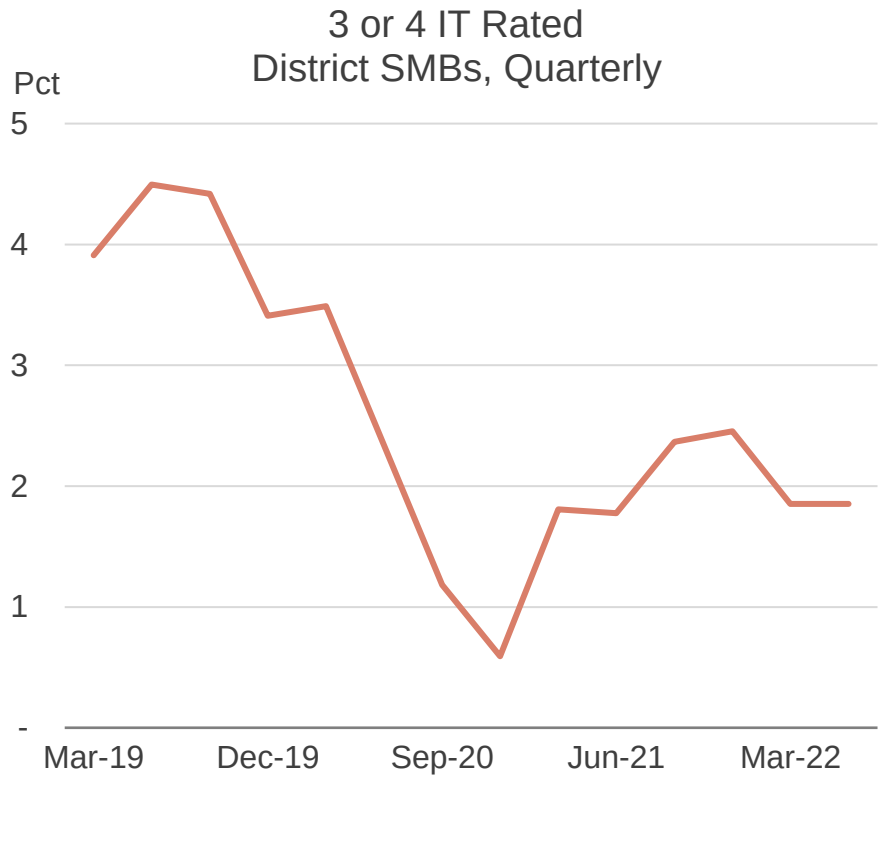
Information Technology and Cybersecurity

Drew Kelley
Manager, Examinations and Inspections

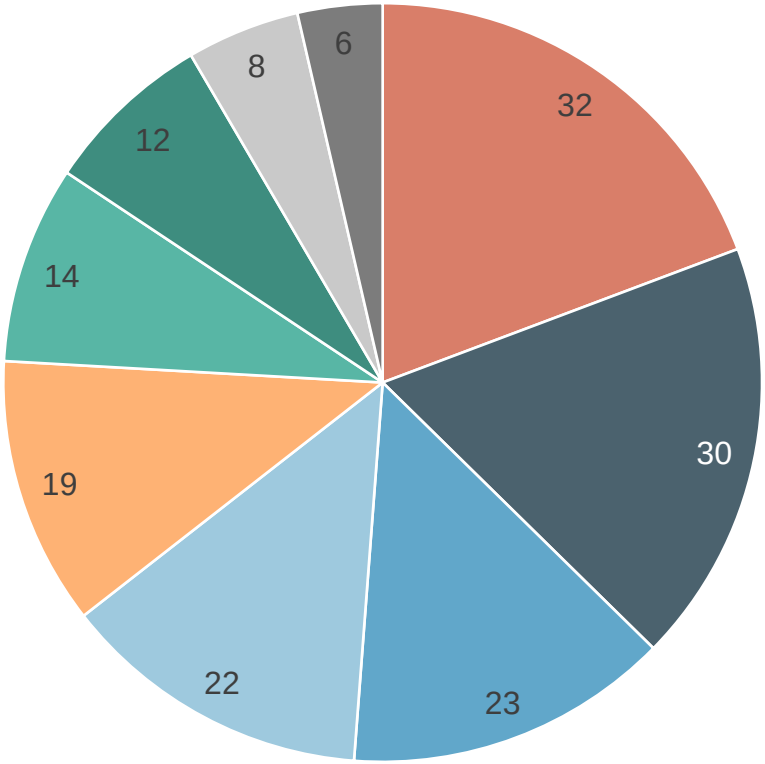
IT Ratings Remain Sound





Source: National Examination Database

Yet IT Findings Are Common



IT-Related Issue Categories
District SMBs, 2019-2022

- Business Continuity/ Incident Response Planning
- User Access
- IT Governance
- IT Audit
- Vendor Risk Management
- Risk Assessment
- Information Security Testing
- Patch Management
- Payments Risk

Source: National Examination Database

Cybersecurity Risk Remains Elevated

- Cyber risk is consistently cited as one of the highest risks to financial institutions.
- Ransomware attacks have grown in sophistication and can happen to any institution or vendor/service provider.
- Financial institutions should be completing cybersecurity assessments and have comprehensive incident response plans.

Critical Risk Management Topics

- Third-Party Risk Management
  - All vendors should be risk-ranked by criticality and procedures should be established and followed for due diligence and ongoing monitoring based on criticality
  - Ongoing vendor monitoring should at a minimum include a review of annual financial performance, technology service provider regulator reports (if available), and a comprehensive review of third-party service provider attestation reports
  - Ensure contractual arrangements contain sufficient language to secure any data that is hosted or processed
  - Consideration should be given to the risk management principles described in SR 13-19, Guidance on Managing Outsourcing Risk

- Patch Management
  - Ensure that known vulnerabilities (especially critical ones) are remediated in a timely manner
  - Consideration should be given to the sound risk management principles documented in the FFIEC IT Handbook on Information Security

Computer-Security Incident Notification Rule

- Financial institutions must notify their primary federal regulator within 36 hours of determining that a notification incident has occurred
- What kind of incident requires notification? An incident that has, or is reasonably likely to, materially disrupt or degrade a bank's:
  - Ability to carry out bank operations, activities, or processes; or deliver products and services to a material portion of its customer base in the normal course of business
  - Business lines, including operations and services that upon failure could result in a material loss of revenue
  - Operations or services, the failure or discontinuance of which would pose a threat to the financial stability of the US
- A bank service provider must notify each affected banking organization customer as soon as possible when the bank service provider determines that it has experienced a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, services provided to such banking organization for four or more hours

Computer-Security Incident Notification Rule

- Financial institutions must notify their primary federal regulator within 36 hours of determining that a notification incident has occurred
- When in doubt, the financial institution is encouraged to still contact their primary federal regulator
- Review Final Rule and SR 22-4
- Contact information for Federal Reserve:
  - Contact your Central Point of Contact (CPC)
  - Contact the Board of Governors by e-mail at incident@frb.gov or phone at (866) 364-0094

Computer-Security Incident Notification Rule

- What kind of incident requires notification? An incident that has, or is reasonably likely to, materially disrupt or degrade a bank's
  - Ability to carry out bank operations, activities, or processes; or deliver products and services to a material portion of its customer base in the normal course of business
  - Business lines, including operations and services that upon failure could result in a material loss of revenue
  - Operations or services, the failure or discontinuance of which would pose a threat to the financial stability of the US

- A bank service provider must notify each affected banking organization customer as soon as possible when the bank service provider determines that it has experienced a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, services provided to such banking organization for four or more hours

Reportable Incident Examples

- Your core banking platform is experiencing a widespread outage and recovery time is unknown
- A failed system upgrade or change results in outages where customers and employees can’t access information
- Your bank experiences a ransomware attack that encrypts system data
- An unrecoverable system failure that results in activation of the institution’s business continuity or disaster recovery plan (may be weather related)

**More examples can be found in the Computer-Security Incident Notification Final Rule*

What To Do If Your Bank Experiences An Incident

- When in doubt, the financial institution is encouraged to contact their primary federal regulator
- Review Final Rule and SR 22-4
- Contact information for Federal Reserve:
  - Contact your Central Point of Contact (CPC)
  - Contact the Board of Governors by e-mail at incident@frb.gov or phone at (866) 364-0094