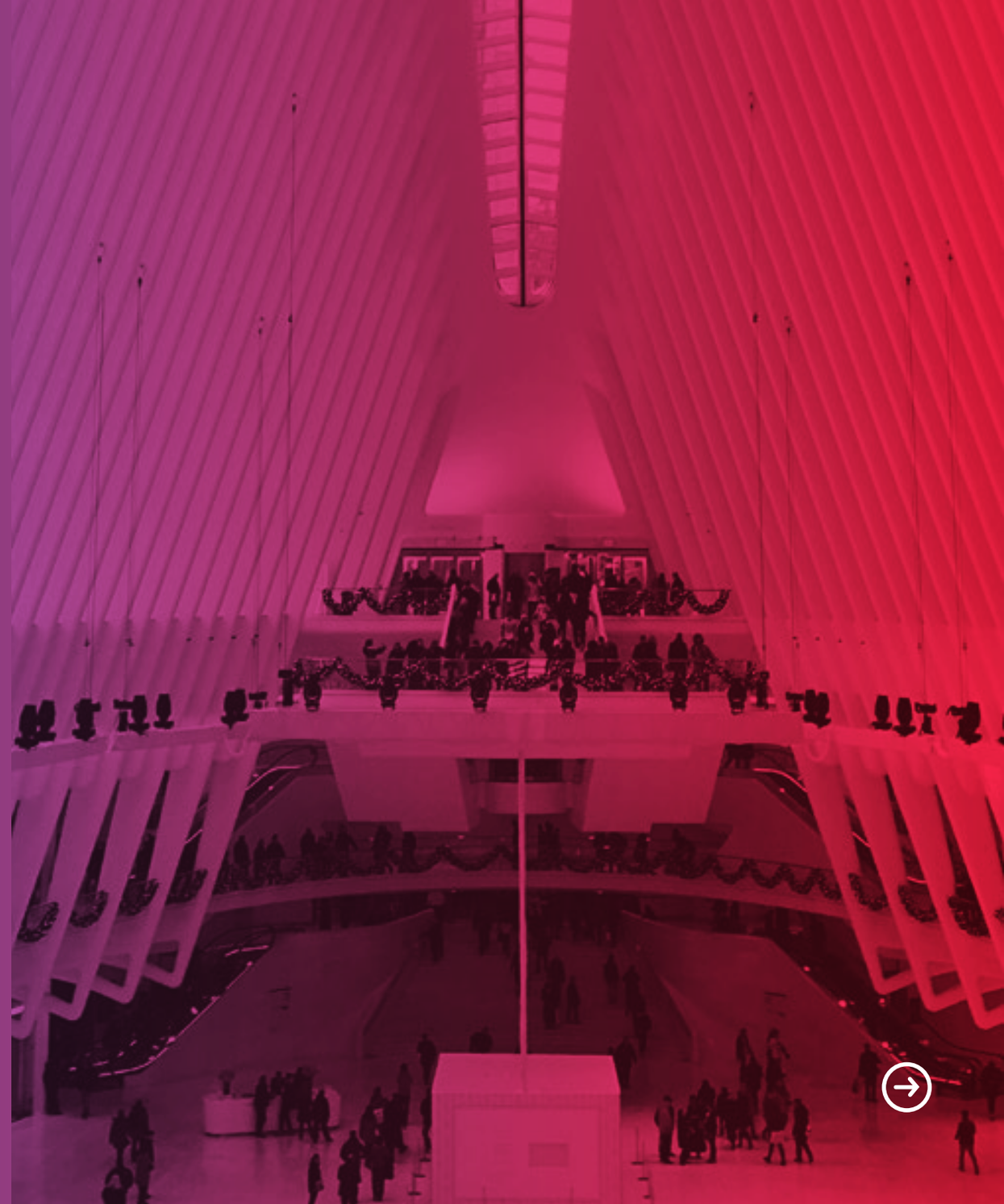
# MANAGED RISK SERVICES

Risk Tools to Help Your Institution Stay Compliant



Many community financial institutions are struggling to stay informed of the federal regulations that are changing so rapidly, to meet the regulator's requests, all the while trying to maintain business as usual. Being proactive is no longer an option, but a necessity. Knowing what resides on the network, having current disaster recovery (DR) plans in place, and managing vendors is an ongoing effort that should be continually reviewed and assessed by the financial institution. A fresh perspective from a third party is sometimes what is needed to stay compliant.

# FIS DELIVERS THE SERVICE AND PARTNERSHIP FINANCIAL INSTITUTIONS CAN RELY ON

Advisory Services, offered through Managed IT Services (MIS), provides financial institutions the opportunity to have a well-seasoned team with banking experience to review the current compliance and regulatory processes in place and provide recommendations.

# SERVICES THAT HELP DRIVE COMPLIANCE

Over the years, these services have been developed, implemented, evaluated, modified and implemented again to ensure the services provided are current with industry and regulatory requirements. The Advisory Services team provides eight different consultative services that have assisted more than 80 community banks annually to meet their regulatory requirements and needs.

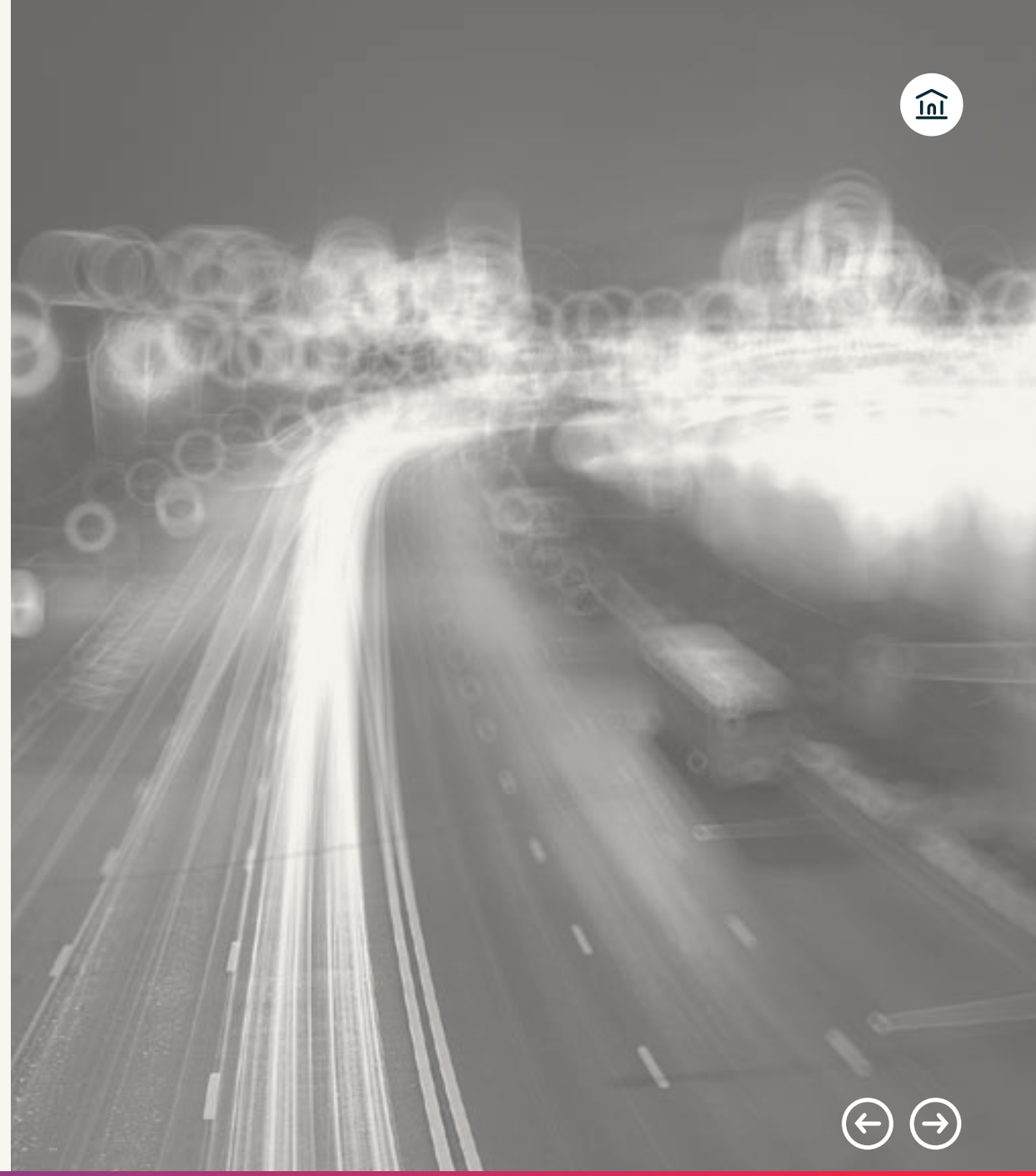
**Managed Risk Services**

- Cybersecurity Risk Assessment
- GLBA Risk Assessment
- Vendor Risk Management
- Business Continuity Plan
- IT DR Walkthrough
- Online Banking Risk Assessment
- Red Flags Risk Assessment
- Enterprise Risk

# CYBERSECURITY RISK ASSESSMENT

Based on the FFIEC's Cybersecurity Assessment Tool (CAT) and the NIST's cybersecurity framework, the Cybersecurity Risk Assessment focuses on the institution's development of a cybersecurity program, protection of systems, detection of threats, response to events and recovery from impact. The service includes:

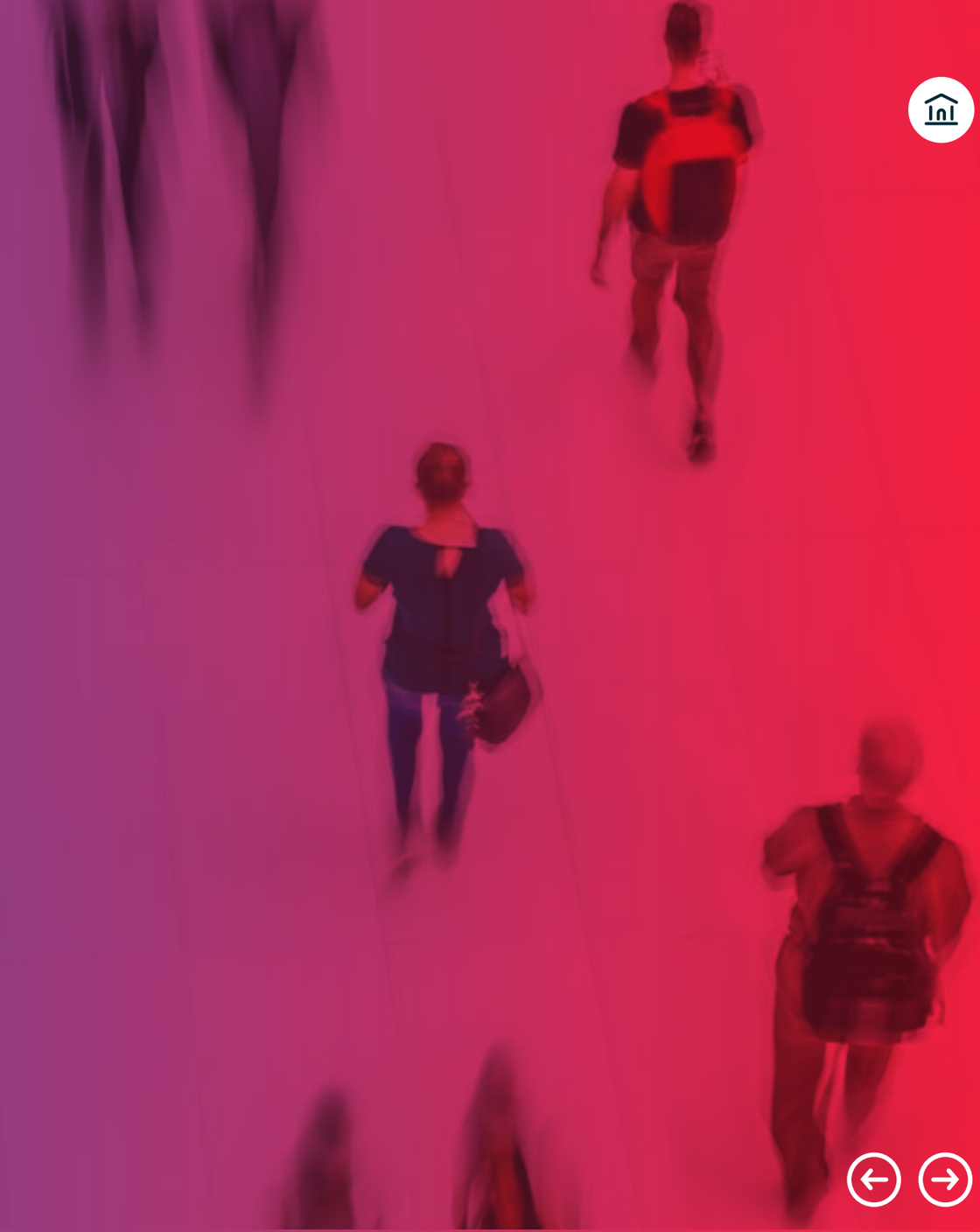
- Executive summary with recommendations
- FFIEC CAT Inherent Risk Profile Review
- FFIEC CAT Cyber Maturity Level Review
- Cybersecurity program review based on the NIST's framework core
- Cybersecurity tier identification and action plan based on the NIST's framework tiers
- Threat analysis that evaluates the risk of different cybersecurity threats
- Controls analysis that evaluates the effectiveness of controls



# GLBA RISK ASSESSMENT

In accordance with the Gramm-Leach-Bliley Act (GLBA), FIS will facilitate the process of gathering information of assets and vendors used and assigning risk ratings to the items discovered. The ranking comprises the following attributes: confidentiality, integrity, availability and the likelihood of these risks. Controls that are in place are also reviewed to mitigate risk to the bank and its customers' data. The service includes:

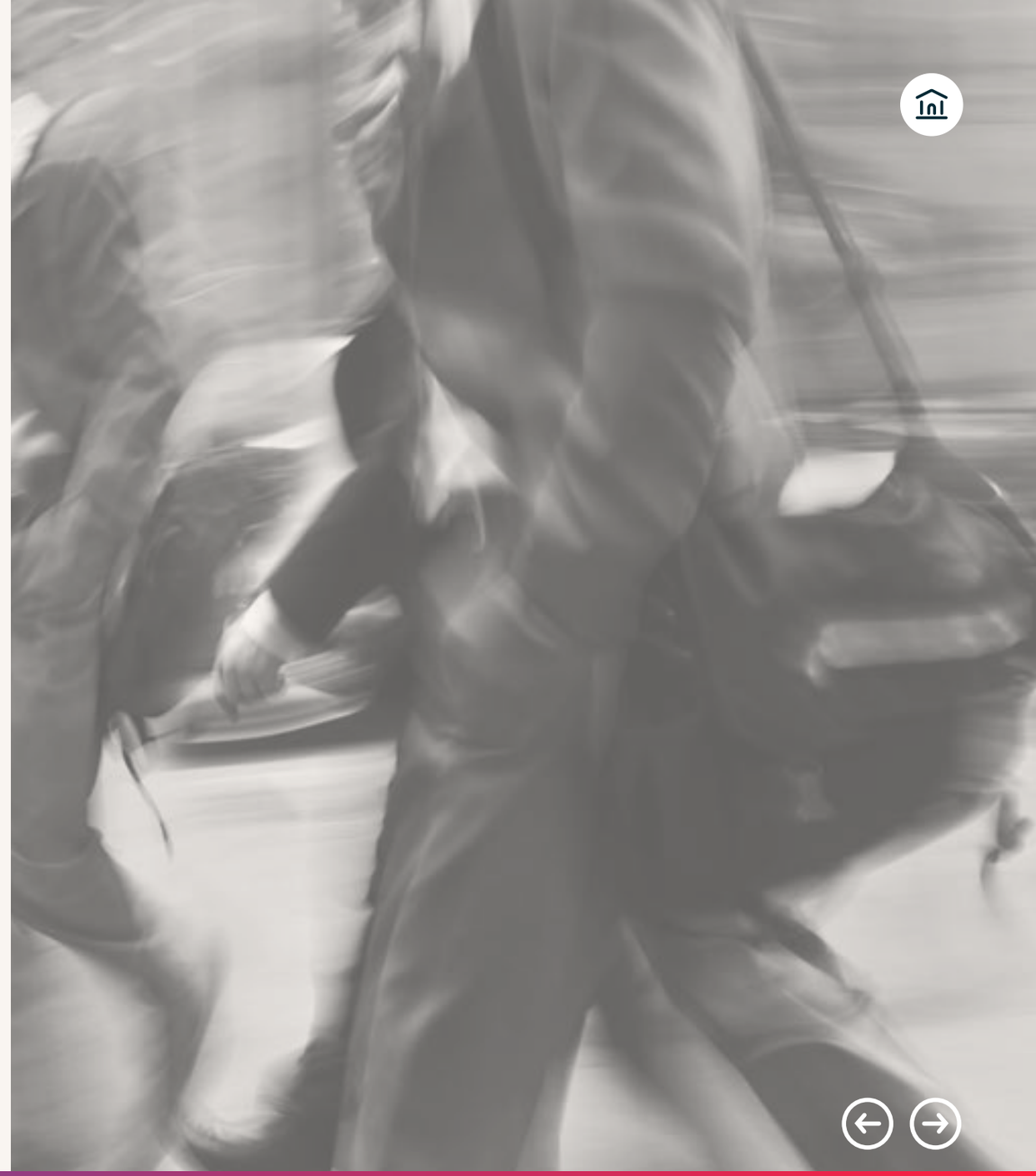
- Executive summary with recommendations
- Asset identification and analysis
- Vendor identification and analysis
- Controls evaluation
- Risks and controls worksheet



# VENDOR RISK MANAGEMENT

This is a facilitated, real-time, online quantitative vendor risk assessment and monitoring service. The service leverages the combination of the ASG facilitative process with the FIS Vendor Risk Manager (VRM) platform that is powered by FIS' Risk as a Service (RaaS). The service includes:

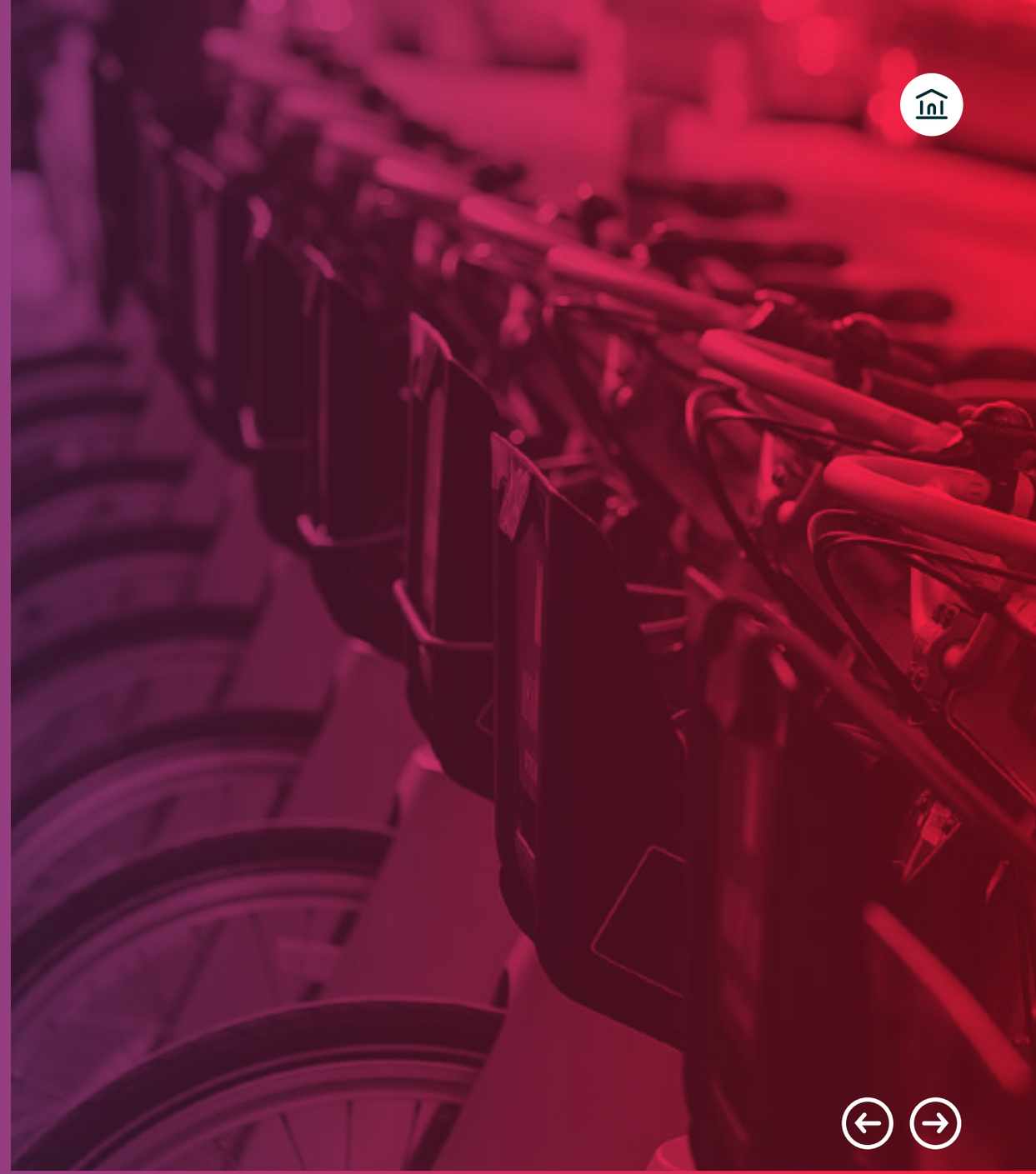
- Facilitated vendor identification and intake rating process
- VRM access integrated within ConnecTED that allows new vendor entries, vendor modifications and monitoring, risk score based on the institution's unique relationship with the vendor, and the complete picture of empirical risk data on the vendor and workflows to review, approve or notify impacted stakeholders of material changes to the vendor's risk profile
- External data feeds that are collected and analyzed by VRM's operational experts
- Vendor due diligence collection and analysis
- Vendor control surveys and analysis



# BUSINESS CONTINUITY PLAN

The intent of this service is to design the financial institution's business continuity plan. The on-site process will identify and train the Crisis Management Team (CMT), establish assembly sites during a disaster, identify missing resources (e.g., DR kits, "go boxes," call tree, etc.) and document the scenario test and results. The business continuity service includes:

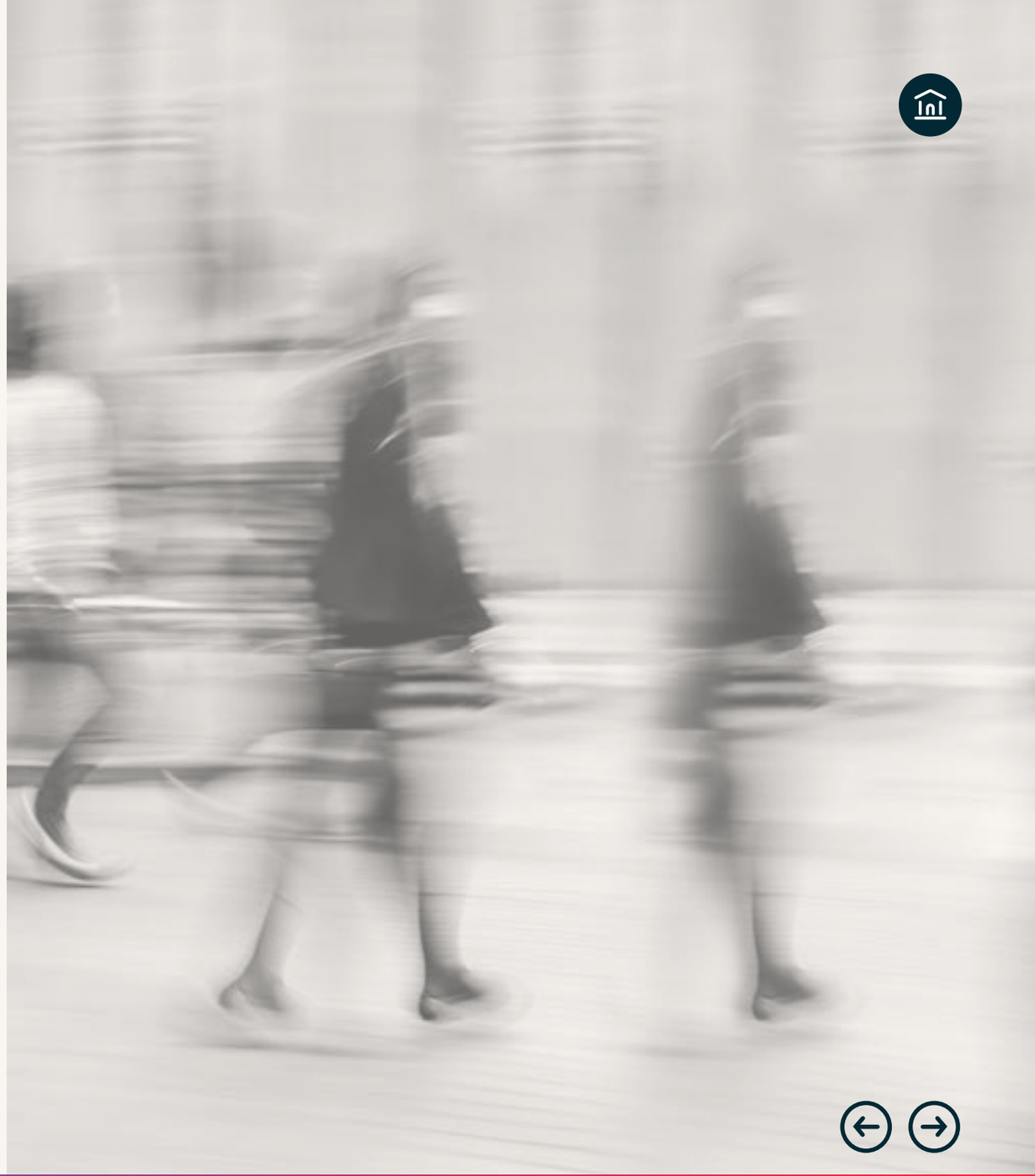
- Business continuity plan
- Business impact analysis
- CMT training
- Documented table top exercise



# IT DR WALKTHROUGH

A technical, documented recovery strategy is created with guidance from FIS engineers. The walkthrough will identify and prioritize recovery efforts and document the business impact during an outage for each piece of equipment. The service includes:

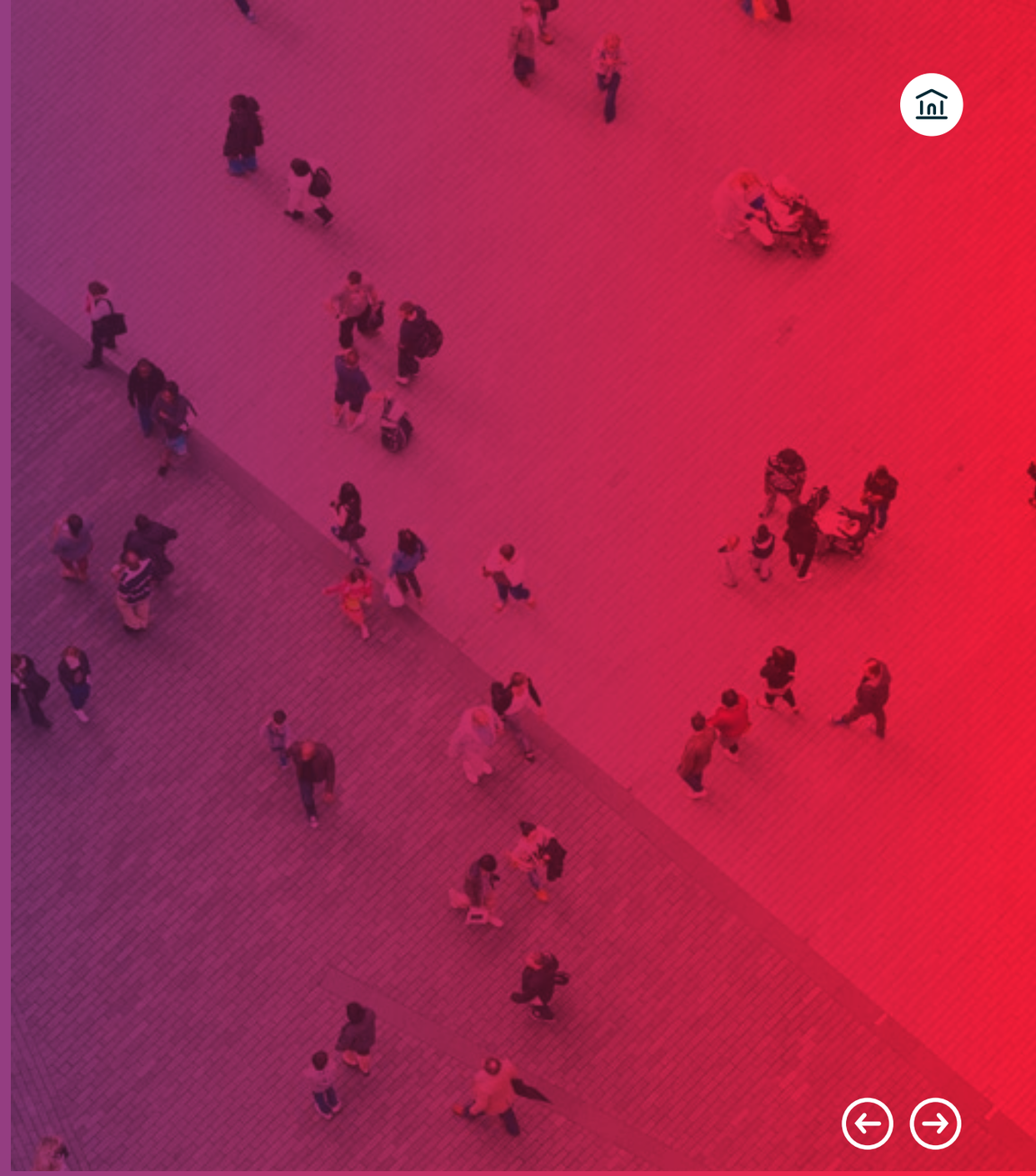
- Documentation on all circuits, infrastructure and servers for business impact during outage, recovery steps and continuation steps during outage
- Network diagram
- Business impact analysis
- Basic DR testing and documentation based on customer needs (additional testing may be completed through a project scope)



# ONLINE BANKING RISK ASSESSMENT

Based on the FFIEC guidance, FIS will facilitate the process of gathering information regarding the financial institution's online banking program, evaluate transaction capability, including assigning risk ratings, and evaluate the controls that are currently in place to mitigate risk. The service includes:

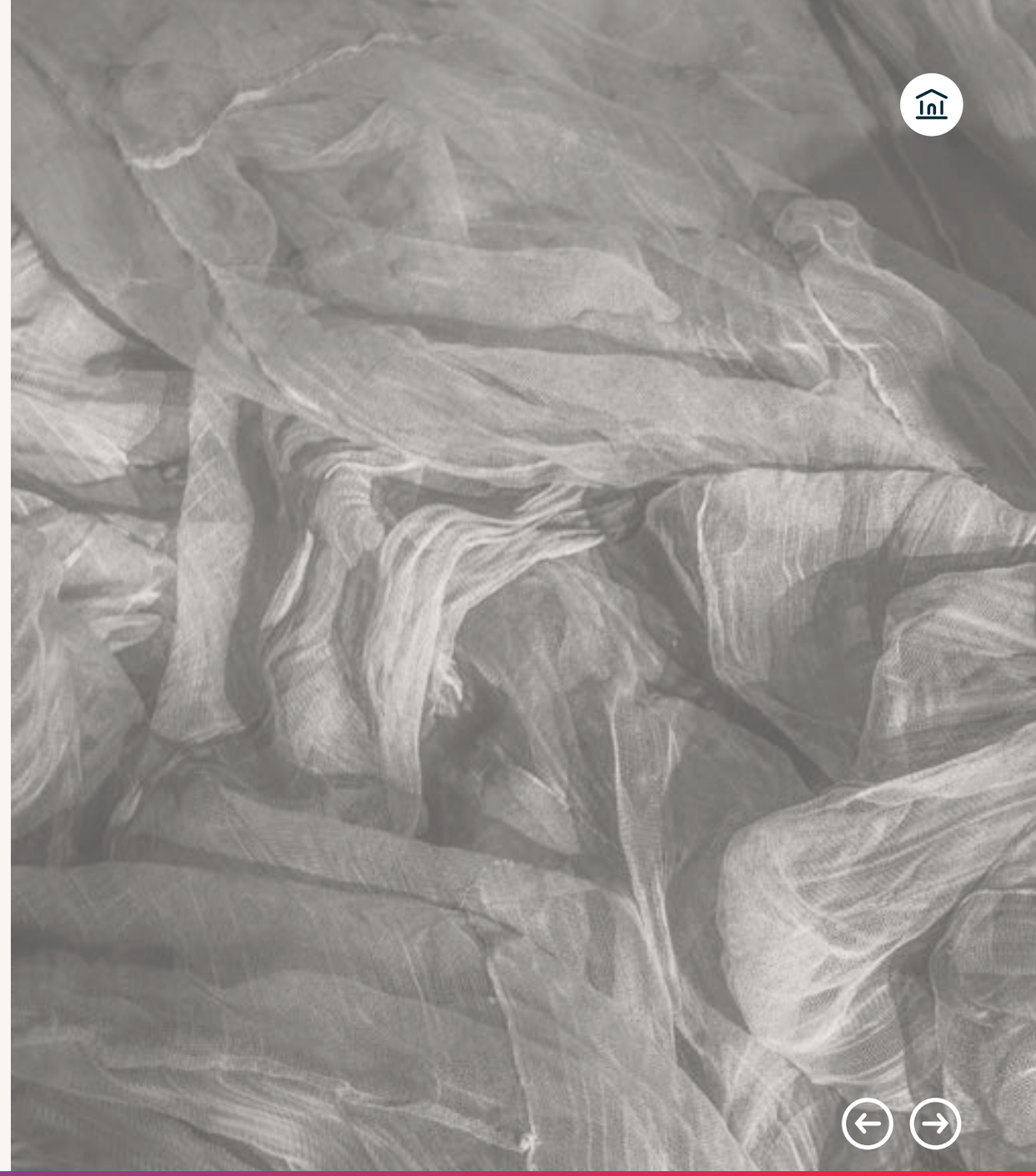
- Executive summary with recommendations
- Program review
- Transaction analysis
- Risk and controls worksheet
- Policy template



# RED FLAGS/ ID THEFT ASSESSMENT

FIS will facilitate the process of identifying all of the financial institution's "covered" accounts and assess the associated risk of ID theft for those accounts. Further review and documentation of the financial institution's processes occurs with the purpose of identifying and detecting the 26 recommended "Red Flags." The service includes:

- Executive summary with recommendations
- Policy template
- Covered account analysis
- Documentation of the financial institution's process to detect, monitor and respond to 26 Red Flags



# ENTERPRISE RISK MANAGEMENT ASSESSMENT

FIS will facilitate the identification and risk rating of all business processes performed by the financial institution. The risk rating process is based on the OCC risk categories, an evaluation of likelihood of risk exposure, and the effectiveness of controls. The analysis will yield an evaluation of enterprise risk, along with departmental risk, in the form of inherent risk, control risk and residual risk. The service includes:

- Executive summary with recommendations
- ERM analysis report
- Bank summary
- Trends analysis
- Risk category analysis
- Departmental analysis
- Risk matrices
- Action items tool