FIS MANAGED RISK SERVICES (MRS)
INTRODUCTION

Financial institutions are struggling to contend with rapidly evolving cybersecurity threats and regulatory/compliance requirements, often lacking clarity about what to do and when.

Many are turning to FIS Managed Risk Services (MRS) to help them stay ahead of the curve.
INTRODUCTION

By partnering with a trusted provider, financial organizations can access…

The expertise
Data-driven insights
And advanced tools

...they need to protect their operations, reputation, and customers from risk now and in the future.
THE TWO MAJOR CHALLENGES FOR US FINANCIAL INSTITUTIONS

In the rush to digital transformation triggered by the pandemic, financial institutions have increased their exposure to two major threat vectors:
The Challenge for US Financial Institutions

1. Increased security breaches

62%

Of all FIs experienced an increase in financial crime in 2022

Source: PMNTS, 2022

$9.44M

Average cost of a data breach in the U.S.

Source: IBM, 2022
THE CHALLENGE FOR US FINANCIAL INSTITUTIONS

2. Increased regulatory/compliance requirements

$4M
In avg. revenue lost due to a single non-compliance event
Source: Secureframe, 2022

170%
More is spent on non-compliance vs compliance
Source: Secureframe, 2022
THE SOLUTION:
FIS MANAGED RISK SERVICES (MRS)
Our Managed Risk Services introduce streamlined management of IT and operational risk for financial organizations:

- **14M+** Deposit accounts vaulted in Sheltered Harbor daily
- **15,000+** Vendors managed for clients
- **5,000** GLBA risk-assessed assets managed for clients
- **400+** Risk advisory services provided to clients
FIS Managed Risk Services Mapped

- Risk management models are based on FFIEC, other regulatory guidance, and industry standards
- Dedicated risk analysts facilitate risk management processes by educating and providing guidance and recommendations
- Our facilitative model allows you to build efficiencies in your risk management processes
- Our team stays current on regulatory expectations to help keep you informed of the ever-changing environment
WHAT MAKES FIS’ MANAGED RISK SERVICES UNIQUE

Designed for financial institutions at their request, our solution stands out in the market due to our people, processes, and tools:

Our people

Because our solution is designed and led by a team of former bankers, we have a unique perspective into how financial organizations operate and what their key needs are.
WHAT MAKES FIS’ MANAGED RISK SERVICES UNIQUE

Designed for financial institutions at their request, our solution stands out in the market due to our people, processes, and tools:

Our processes

We constantly monitor for changes in the regulatory environment and collaborate with our clients’ auditors and examiners to stay ahead of trends and deliver up-to-date compliance and best practice guidance to customers.
WHAT MAKES FIS’ MANAGED RISK SERVICES UNIQUE

Designed for financial institutions at their request, our solution stands out in the market due to our people, processes, and tools:

Our tools

We offer you the same cutting-edge risk management and assessment toolset that we use to protect ourselves – ensuring you have a successful risk, information security, and compliance program at your fingertips.
Enhancing compliance, continuity, and security, you can pick and choose from our range of MRS core offerings.
Our assessment and monitoring service offers a customized risk score based on your unique relationship with each of your vendors. All data feeds are analyzed by our experts who provide you with greater financial health, PCI, regulatory, and consumer compliance awareness.

FIS collects, reviews, and delivers custom control surveys and provides reviews of any supporting documentation.
Gain access to a centralized system for reporting, evidence/contract storage, issue management, and automated workflows.

Benefit from news sentiment analysis for up-to-date awareness of any negative news on your vendors.

Tracking of Service Level Agreements (SLAs) and Key Performance Indicators (KPIs) monitored.
RED FLAGS RISK ASSESSMENT

Key features

Risks assessed
Dedicated risk analyst conducts an assessment to identify all ‘covered’ and ‘non-covered’ accounts and evaluate their risk of identity theft.

Flags surveyed
Analyst also carries out a review of numerous Red Flag indicators, including the 26 FFIEC indicators.

Gaps identified
Detection and response processes are applied to each Red Flag situation, documented, and assessed to determine if there are any process gaps.
Transaction analysis based on the FFIEC Internet Banking Guidance calculates inherent/residual risk scores, including which transactions pose the greatest risk.

**Key features**

**Improvement focused**
Dedicated risk analyst introduces risk assessment processes and creates documentation with recommendations on program/process improvements.

**Risk scored**
Transaction analysis based on the FFIEC Internet Banking Guidance calculates inherent/residual risk scores, including which transactions pose the greatest risk.

**Blindspots revealed**
Program review conducted based on FFIEC Internet Banking Guidance to identify any online banking program gaps.

**Processes reviewed**
Review of online banking risks, identification, documentation, and controls evaluation to identify process gaps.
Data is analyzed to provide an overview based on the organization, each department, and each risk category. Trend analysis is also performed if multiple years of data are available.

**Key features**

**Every department covered**
- Dedicated risk analyst conducts sessions with each business unit/department

**Data deciphered**
- Data is analyzed to provide an overview based on the organization, each department, and each risk category. Trend analysis is also performed if multiple years of data are available

**Business profiled**
- Enterprise assessment identifies all business functions and associated risk before evaluating the impact based on the nine OCC risk categories and the effectiveness of physical, technical, and administrative controls

**Risks prioritized**
- Action items list developed to precisely evaluate high risk areas and determine whether they are within an acceptable risk tolerance or if an action plan is required
DATA RESTORE

Key features

Data shielded
File creation, validation, encryption, and vaulting service that backs up your account data offline and provides a comprehensive recovery process

Certification accelerated
Accelerated qualification for the Sheltered Harbor Data Protection certification that ensures you are vaulted, coordinates the data verification test, and guides you through the certification process

Sheltered Harbor secured
Membership to the Sheltered Harbor community with exclusive access to materials and best practices for data protection and recovery
Our Disaster Analysis service examines different disaster threats and their potential impact as well as the likelihood of occurrence.

**Disaster avoided**
Our Disaster Analysis service examines different disaster threats and their potential impact as well as the likelihood of occurrence.

**Risk audited**
Dedicated risk analyst and a network engineer review each circuit, infrastructure device, and server, documenting the business impact of an outage while detailing potential outage procedures and recovery strategies.

**Impact profiled**
Our facilitated Business Impact Analysis (BIA) identifies dependencies, Recovery Time Objectives (RTOs), and Recovery Point Objectives (RPOs).

**Recovery formalized**
FIS’ DR Testing collects and formalizes technical DR testing documentation.
As with our Disaster Recovery offering, FIS identifies dependencies, RTOs, and RPOs and conducts full Disaster Analysis.

**Key features**

**Planning updated**
Dedicated risk analyst leads the collection of information required for the development and maintenance of your business continuity plan, incorporating changes to meet current regulatory expectations.

**Dependencies determined**
As with our Disaster Recovery offering, FIS identifies dependencies, RTOs, and RPOs and conducts full Disaster Analysis.

**Scenarios tested**
Documented tabletop exercise covering three disaster scenarios including physical disaster, pandemic, and cyber attack.
FIS follows a three-step process to source the intelligence your organization needs to combat risk:

1. **Identify**
   Understand risks from social/digital platforms, deep/dark web, mobile app stores, and more

2. **Protect**
   Defend brand, products, execs, financial accounts, payment cards, and other monetary assets

3. **Remediate**
   Counteract threats to your brand, business, and the financial accounts of your customers
**Key criteria**

**FFIEC CAT Inherent Risk Profile**
Assessment based on the 39 FFIEC Inherent Risk areas and their scoring methodology

**FFIEC CAT Maturity Level**
Comprehensive review of the ~500 declarative statements with risk analysts providing clarity, peer perspectives, and recommendations on how to achieve a desired maturity level

**NIST Cybersecurity Framework Core**
Inherent risk, residual risk, and controls identification based on the National Institute of Standards & Technology (NIST) Cybersecurity Framework Core

**NIST Cybersecurity Framework Tiers**
Evaluation of cybersecurity maturity based on the NIST Cybersecurity Framework Tiers

**Cyber Threat Analysis**
Assessment of the financial, reputational, legal/regulatory, operational impact, and likelihood of various cyber threats combined with full controls identification and evaluation
GLBA RISK MANAGER (GRM)

Key features

Risk reviewed
Real-time, online quantitative risk assessment and monitoring service with customized score based on your GLBA risk

Issues managed
Launch issues and associate them to an asset; control whether each issue is identified during testing, during normal operations of an asset, or by an auditor/examiner

Controls checked
Schedule, coordinate, and manage controls testing as well as assign test owners, define testing plans, upload evidence, and document results

Scores updated
Once found, an issue dynamically impacts the residual risk score of the asset, reducing the risk mitigation rating for the corresponding control until the issue is resolved
**Key features**

**Awareness increased**
Running 36 campaigns a year, three campaigns a month, to build security awareness across your organization.

**Campaigns targeted**
General campaigns to capture metrics and build overall awareness as well as targeted campaigns featuring tailored content aimed at designated business units.

**Education enhanced**
Videos, newsletters, and quizzes to enhance cybersecurity education and awareness.

**Security probed**
Reporting metrics to analyze company security effectiveness and identify areas of weakness.

**Plugin provided**
Our integrated Microsoft Outlook/Exchange plugin enables end users to report suspicious emails in seconds.
SECURE YOUR FINANCIAL ORGANIZATION

From internal and external risks with FIS Managed Risk Services. Learn more about how we can help you manage the risks of today and tomorrow:


Email: getinfo@fisglobal.com
ALTERNATIVELY, CONTACT YOUR RELATIONSHIP MANAGER TO DISCUSS YOUR SECURITY AND RISK REQUIREMENTS:

Contact: https://www.fisglobal.com/en/contact-us / Email: getinfo@fis.com