Data Edge Pro

White Paper

FINMA Circular 2023/1

Mastering Critical Data Risk Management

A Comprehensive Implementation Guide for Swiss Financial Institutions

By Bernard Millet

Data Management & Governance expert

April 2025

Executive Summary

The Swiss Financial Market Supervisory Authority's (FINMA) Circular 2023/1 "Operational Risks and Resilience - Banks" represents a pivotal shift in regulatory expectations for financial institutions operating in Switzerland.

Coming into force on January 1, 2024, with a compliance deadline of June 1, 2024, this comprehensive framework significantly enhances requirements for operational resilience with particular emphasis on critical data risk management.

This whitepaper provides a structured analysis of the new requirements, examining implementation challenges and opportunities across various organizational roles. Financial institutions must now adopt a systematic approach to identifying, classifying, and protecting critical data throughout its lifecycle.

Organizations that view this regulatory shift as a strategic opportunity rather than a compliance burden will realize substantial benefits: enhanced operational resilience, improved data governance, strengthened cybersecurity posture, and increased stakeholder trust.

This paper offers a practical roadmap for implementation, outlining key responsibilities for C-suite executives, IT professionals, compliance officers, risk managers, and finance leaders.

Table of Contents

Executive Summary 2
Introduction 4
Key Challenges and Opportunities 5
For C-Suite Executives 6
For IT Professionals 8
For Compliance Officers 10
For Risk Managers 12
For Finance Leaders 13
Strategic Framework 15
Implementation Approach 18
Best Practices and Recommendations 21
Key Performance Indicators 22
Conclusion 23
References 24

Introduction

In December 2022, FINMA published Circular 2023/1 "Operational Risks and Resilience - Banks," replacing the previous Circular 2008/21 on operational risks. This regulatory evolution reflects the rapidly changing digital landscape and the growing importance of data as a critical asset in the financial sector. The new circular introduces comprehensive requirements for operational resilience, with specific focus on critical data risk management.

Critical data, defined as information essential for the successful and sustainable provision of an institution's services or required for regulatory purposes, has emerged as a foundational element of institutional resilience. The confidentiality, integrity, and availability of this data must be ensured through robust governance frameworks, technical controls, and organizational measures.

This shift comes at a crucial time for the financial industry. As institutions increasingly digitize operations and leverage advanced technologies like cloud computing, artificial intelligence, and big data analytics, the volume and complexity of critical data are growing exponentially. Simultaneously, cyber threats are becoming more sophisticated, making data protection a strategic imperative rather than a technical concern.

The business case for effective critical data risk management extends beyond compliance. Organizations that implement robust frameworks can expect improved operational efficiency, enhanced decision-making capabilities, strengthened customer trust, and increased competitive advantage. Conversely, inadequate data risk management can lead to significant operational disruptions, regulatory penalties, reputational damage, and financial losses.

This whitepaper provides a comprehensive guide to understanding and implementing the critical data risk management requirements of FINMA Circular 2023/1, offering insights for all key stakeholders involved in the compliance journey.

Key Challenges and Opportunities

Challenges

- **Challenge 1: Data Identification and Classification**
  Identifying critical data across complex organizational structures and legacy systems requires significant effort. Many institutions lack a comprehensive inventory of their data assets, making classification a challenging first step.
- **Challenge 2: Governance Integration**
  Aligning critical data risk management with existing governance frameworks requires coordinated effort across multiple organizational functions, including IT, compliance, risk management, and business units.
- **Challenge 3: Technical Implementation**
  Implementing appropriate technical controls for data protection across diverse IT landscapes, including legacy systems, cloud environments, and third-party services, presents substantial complexity.

Opportunities

- **Opportunity 1: Enhanced Operational Resilience**
  The systematic approach to critical data management strengthens overall operational resilience, reducing the likelihood and impact of data-related incidents.
- **Opportunity 2: Improved Data Governance**
  The requirements drive organizations to develop more mature data governance capabilities, which can be leveraged for broader business value beyond compliance.
- **Opportunity 3: Competitive Differentiation**
  Organizations that excel in critical data risk management can differentiate themselves in the marketplace through enhanced customer trust and operational excellence.

For C-Suite Executives

The FINMA Circular 2023/1 presents strategic implications that extend beyond mere compliance. For C-suite executives, this regulatory shift represents an opportunity to strengthen organizational resilience while driving digital transformation initiatives.

Business Value Drivers

- **Operational Resilience Enhancement**: By identifying and protecting critical data, organizations can minimize the impact of operational disruptions, ensuring business continuity in challenging environments.
- **Strategic Risk Reduction**: A comprehensive approach to critical data risk management reduces the likelihood of significant operational, reputational, and financial impacts from data incidents.
- **Digital Transformation Enablement**: Proper management of critical data creates a foundation for leveraging data assets in digital transformation initiatives, enhancing competitive positioning.

Executive Sponsorship

C-suite executives must take active roles in critical data risk management:

- **CEO**: Establish critical data protection as a strategic priority and ensure sufficient resources are allocated for implementation.
- **CIO/CTO**: Oversee technical architecture and controls for critical data protection.
- **CISO**: Lead the development of security frameworks for critical data.
- **COO**: Ensure operational processes integrate critical data risk management practices.
- **CFO**: Evaluate investment requirements and long-term financial benefits.

Investment Considerations

Investment Area	Description	Typical ROI Timeframe
Data Discovery Tools	Technologies to identify and classify critical data across the organization	12-18 months
Protection Technologies	Implementation of technical controls for data protection	18-24 months

Investment Area	Description	Typical ROI Timeframe
Governance Enhancement	Development of policies, procedures, and organizational structures	12-18 months

Source: McKinsey & Company, "Operational Resilience in Financial Services" (2023)

Executive Takeaway

FINMA Circular 2023/1 requires executive commitment to critical data risk management as a strategic initiative rather than a compliance exercise. By establishing clear accountability at the executive level, allocating appropriate resources, and integrating critical data considerations into strategic planning, organizations can transform regulatory requirements into business value. The circular's implementation deadline of June 1, 2024, necessitates immediate action to ensure compliance and realize the potential competitive advantages.

For IT Professionals

IT professionals face the technical challenge of implementing robust critical data protection measures across diverse technology landscapes while ensuring operational efficiency and user experience.

Technical Architecture Components

An effective critical data risk management framework requires several integrated technical components:

- **Data Discovery and Classification**: Automated tools to identify, classify, and tag critical data across storage locations.
- **Access Control Systems**: Role-based access controls with strong authentication mechanisms.
- **Data Protection Technologies**: Encryption, tokenization, and data loss prevention solutions.
- **Monitoring and Detection**: Real-time monitoring of critical data access and usage patterns.
- **Incident Response Tools**: Automated workflows for critical data incidents.

Implementation Considerations

- **Data Discovery**: Implement tools capable of scanning structured and unstructured data across on-premises and cloud environments. Focus on accuracy and coverage while minimizing performance impact.
- **Protection Mechanisms**: Deploy layered security controls based on data classification. Implement encryption for data at rest and in transit, with particular attention to key management. Establish data loss prevention mechanisms for critical data exfiltration detection.

Technology Evaluation Criteria

1. Scalability across diverse technology environments
2. Integration capabilities with existing security infrastructure
3. Automation capabilities to reduce manual effort
4. Performance impact on business operations
5. Reporting capabilities for compliance demonstration

IT Professional Takeaway

The technical implementation of FINMA Circular 2023/1 requires a systematic approach to critical data management across the entire technology stack. Begin with a comprehensive data discovery exercise to identify critical data repositories, then implement appropriate classification mechanisms. Leverage automation where possible to reduce manual effort, particularly for ongoing monitoring and reporting. Focus on building a flexible architecture that can adapt to changing business needs and threat landscapes while maintaining compliance with regulatory requirements.

For Compliance Officers

Compliance officers must ensure that the organization's critical data risk management framework meets FINMA requirements while integrating with the broader regulatory compliance landscape.

Key Regulations

Regulation/Standard	Geographic Scope	Key Requirements
FINMA Circular 2023/1	Switzerland	Critical data identification, classification, protection, and monitoring
GDPR	European Union	Protection of personal data, data subject rights, breach notification
Swiss Data Protection Act	Switzerland	Protection of personal data, transparency, security requirements
ISO 27001	International	Information security management system requirements

Source: KPMG, "Regulatory Landscape for Financial Services in Switzerland" (2023)

Compliance Controls

- **Governance Controls**: Establish clear policies, procedures, and responsibilities for critical data management. Implement regular reporting to executive management and the board.
- **Operational Controls**: Develop procedures for critical data identification, classification, protection, and monitoring. Implement documentation requirements for control effectiveness.
- **Technical Controls**: Ensure that technical measures for critical data protection align with regulatory requirements and industry standards.

Compliance Officer Takeaway

The critical data risk management requirements in FINMA Circular 2023/1 represent a significant enhancement of regulatory expectations. Compliance officers should develop a comprehensive control framework that addresses all aspects of the circular, with particular attention to governance structures, data management processes, and

technical protection measures. Focus on creating clear documentation that demonstrates compliance with both the letter and spirit of the regulation. Regular assessments and gap analyses will be essential to maintain compliance, especially as the regulatory landscape continues to evolve.

For Risk Managers

Risk managers must integrate critical data considerations into the enterprise risk management framework, ensuring that data-related risks are identified, assessed, and mitigated appropriately.

Key Risk Categories

- **Data Confidentiality Risk**: Unauthorized access to critical data resulting in competitive disadvantage, legal liability, or reputational damage.
- **Data Integrity Risk**: Corruption or unauthorized modification of critical data leading to operational disruptions, financial losses, or regulatory non-compliance.
- **Data Availability Risk**: Inability to access critical data when needed, resulting in business process disruptions, customer service impacts, or compliance failures.
- **Third-Party Risk**: Vulnerabilities introduced through service providers or vendors with access to critical data.

Mitigation Strategies

- **Risk Assessment Framework**: Develop a structured approach to evaluating critical data risks, considering likelihood, impact, and existing controls.
- **Risk Register Development**: Create and maintain a comprehensive register of critical data risks, with clear ownership and mitigation plans.
- **Control Effectiveness Testing**: Regularly evaluate the effectiveness of controls protecting critical data, including technical measures and procedural safeguards.
- **Scenario Analysis**: Conduct regular scenario planning exercises to assess organizational readiness for different critical data risk events.

Risk Manager Takeaway

FINMA Circular 2023/1 requires a robust risk management approach to critical data that extends beyond technical controls to encompass governance, process, and people aspects. Risk managers should lead the development of comprehensive risk assessment methodologies specific to critical data, ensuring that risks are properly identified, evaluated, and mitigated. Regular reporting to the board and executive management on critical data risks and control effectiveness will be essential for maintaining strong governance. Integration with enterprise risk management frameworks will ensure that critical data risks are considered alongside other strategic and operational risks.

For Finance Leaders

Finance leaders must balance the investment required for critical data risk management against the potential financial benefits and risk reduction.

Cost Structure Overview

Cost Category	Year 1	Year 2	Year 3
Initial Investment	CHF 400,000-800,000	CHF 200,000-400,000	CHF 100,000-200,000
Implementation	CHF 300,000-600,000	CHF 200,000-400,000	CHF 100,000-200,000
Ongoing Operations	CHF 200,000-400,000	CHF 300,000-500,000	CHF 300,000-500,000

Source: Deloitte's 2023 Financial Services Implementation Study[1] and PwC's 2023 Banking Compliance Cost Analysis[2]

Financial Benefits

- **Direct Benefits:**
    - Reduced operational losses from data incidents (estimated at 15-30% reduction, per IBM Cost of Data Breach Report 2024[3])
    - Lower remediation costs for data breaches or corruption (estimated at 20-40% reduction, according to Ponemon Institute's 2023 Cost of Compliance Study[4])
    - Decreased audit and compliance costs through efficient processes (estimated at 10-20% reduction, based on EY Financial Services Regulatory Technology Survey 2023[5])
- **Indirect Benefits:**
    - Enhanced operational efficiency through improved data management
    - Reduced opportunity costs from operational disruptions
    - Potential competitive advantage through strengthened customer trust

Finance Leader Takeaway

While the implementation of critical data risk management requirements represents a significant investment, the financial benefits extend beyond risk reduction. Finance leaders should adopt a total cost of ownership approach that considers both

implementation costs and ongoing operational expenses. Develop a detailed business case that quantifies the benefits of critical data risk management, including reduced operational losses, lower remediation costs, and enhanced business capabilities. Consider innovative funding approaches that distribute costs across multiple business initiatives, particularly where critical data management capabilities support broader digital transformation goals.

Strategic Framework

A comprehensive framework for critical data risk management under FINMA Circular 2023/1 must integrate governance, process, and technology elements into a cohesive approach. The following framework provides a structured approach to implementing the circular's requirements.

Framework Components

1. Governance and Organization

The foundation of effective critical data risk management lies in clear governance structures and defined responsibilities. This component includes:

- Executive board-level sponsorship and oversight
- Dedicated unit responsible for critical data framework development and monitoring
- Clear roles and responsibilities across the organization
- Integration with enterprise risk management and information security governance
- Regular reporting mechanisms to senior management and the board

Implementation considerations include defining the appropriate organizational structure based on the institution's size and complexity, establishing reporting lines that ensure independence, and developing metrics that enable effective oversight.

2. Critical Data Lifecycle Management

This component addresses the management of critical data throughout its lifecycle, from creation to deletion:

- Comprehensive data inventory and classification methodology
- Data discovery and classification processes
- Protection requirements based on classification levels
- Data retention and disposal policies
- Integration with change management processes

Implementation considerations include developing classification criteria that balance granularity with usability, implementing automated discovery tools where appropriate, and establishing regular review cycles to ensure ongoing accuracy.

3. Risk and Control Framework

The risk and control framework provides the structure for identifying, assessing, and mitigating critical data risks:

- Risk assessment methodology for critical data
- Control catalog mapping to specific risks
- Control testing and monitoring processes
- Incident management procedures
- Integration with business continuity planning

Implementation considerations include developing risk scenarios specific to different types of critical data, establishing appropriate risk appetites, and implementing preventive, detective, and corrective controls.

4. Technical Protection Measures

This component encompasses the technical controls required to protect critical data:

- Access control mechanisms based on least privilege principles
- Encryption for data at rest and in transit
- Data loss prevention capabilities
- Monitoring and alerting systems
- Backup and recovery mechanisms

Implementation considerations include selecting technologies that integrate with existing infrastructure, establishing appropriate key management processes, and developing monitoring capabilities that balance security with privacy requirements.

5. Third-Party Risk Management

This component addresses the risks associated with third parties that access, process, or store critical data:

- Due diligence procedures for third-party assessment
- Contractual requirements for critical data protection
- Ongoing monitoring and reassessment processes
- Exit strategies for critical data retrieval

Implementation considerations include developing risk-based approaches to third-party assessment, establishing clear contractual obligations, and implementing monitoring mechanisms for ongoing compliance.

6. Training and Awareness

This component focuses on building a culture of data protection across the organization:

- Role-based training programs for staff handling critical data
- Awareness campaigns for all employees
- Specialized training for technical and security personnel
- Integration with performance management systems

Implementation considerations include developing engaging training content, establishing mechanisms to measure training effectiveness, and creating incentives for compliance with critical data protection requirements.

The success of this framework depends on the integration of these components into a cohesive approach that is proportionate to the institution's size, complexity, and risk profile. Regular assessment and refinement of the framework will ensure ongoing alignment with regulatory expectations and evolving best practices.

Implementation Approach

Implementing FINMA Circular 2023/1 critical data risk management requirements requires a structured approach that balances thoroughness with time constraints, given the June 1, 2024 compliance deadline.

Implementation Phases

Phase 1: Assessment and Planning (2-3 months)

- **Focus Areas:**
  - Gap analysis against FINMA requirements
  - Current state assessment of critical data practices
  - Development of implementation roadmap
- **Key Deliverables:**
  - Detailed gap analysis report
  - Implementation plan with resource requirements
  - Executive sponsorship and governance structure

Phase 2: Foundation Building (3-4 months)

- **Focus Areas:**
  - Establishing governance structures
  - Developing policies and procedures
  - Implementing basic technical controls
- **Key Deliverables:**
  - Critical data governance framework
  - Core policy documentation
  - Initial critical data inventory methodology

Phase 3: Critical Data Identification and Classification (3-4 months)

- **Focus Areas:**
  - Critical data discovery across the organization
  - Application of classification methodology
  - Documentation of critical data inventory

- **Key Deliverables:**
    - Comprehensive critical data inventory
    - Classification of identified critical data
    - Initial risk assessment of critical data assets

Phase 4: Protection Implementation (4-6 months)

- **Focus Areas:**
    - Implementation of technical controls
    - Development of monitoring capabilities
    - Integration with incident response processes
- **Key Deliverables:**
    - Access control mechanisms for critical data
    - Encryption implementation for high-risk data
    - Monitoring and alerting capabilities

Phase 5: Testing and Validation (2-3 months)

- **Focus Areas:**
    - Control effectiveness testing
    - Scenario-based testing
    - Documentation of control environment
- **Key Deliverables:**
    - Test results and remediation plans
    - Updated risk assessments
    - Compliance documentation package

Phase 6: Continuous Improvement (Ongoing)

- **Focus Areas:**
    - Regular assessment of control effectiveness
    - Adaptation to changing business needs
    - Integration of emerging best practices
- **Key Deliverables:**

    - Ongoing monitoring reports
    - Periodic review of critical data inventory
    - Continuous improvement initiatives

Key Stakeholders and Resources

Stakeholders:

- Executive board and senior management
- Information security team
- IT department
- Risk management function
- Compliance department
- Business unit representatives
- Data owners and stewards
- Internal audit

Resources Required:

- Executive sponsorship
- Dedicated project team
- Subject matter experts in data management and security
- Technical resources for implementation
- Budget for tools and technologies
- External consultants (if needed)

The implementation approach should be tailored to the specific characteristics of the organization, including size, complexity, existing capabilities, and risk profile. Smaller institutions may combine phases or leverage external resources to accelerate implementation, while larger organizations may need a more comprehensive approach with multiple workstreams.

Best Practices and Recommendations

Based on early implementation experiences and industry best practices, the following recommendations can help organizations successfully implement FINMA Circular 2023/1 critical data risk management requirements:

1. **Start with a Comprehensive Data Discovery Exercise**
   Before implementing classification schemes or protection measures, invest in thorough data discovery across all repositories. Use automated tools where possible, but recognize that manual input from business units will be essential for accurate identification of critical data.

2. **Adopt a Risk-Based Approach to Implementation**
   Focus initial efforts on the most critical data elements, ensuring that high-risk data receives appropriate protection early in the implementation process. This approach balances resource constraints with risk reduction goals.

3. **Integrate Critical Data Management with Existing Processes**
   Avoid creating parallel processes for critical data management. Instead, integrate requirements into existing risk management, information security, and data governance frameworks to enhance efficiency and effectiveness.

4. **Implement "Defense in Depth" for Critical Data Protection**
   Develop layered protection mechanisms that include technical controls, procedural safeguards, and awareness programs. This approach ensures that the failure of any single control does not compromise critical data security.

5. **Establish Clear Metrics and Reporting Mechanisms**
   Develop meaningful metrics that measure both compliance with requirements and the effectiveness of controls. Regular reporting to management and the board will ensure continued focus on critical data protection.

Key Performance Indicators

Category	Metric	Description	Target
Governance	Critical Data Governance Maturity	Assessment of governance framework maturity using a defined scale	Level 4 (out of 5)[6]
Data Management	Critical Data Coverage	Percentage of systems scanned for critical data	100%[7]
Data Management	Classification Accuracy	Percentage of data correctly classified as verified by sampling	>95%[7]
Protection	Access Control Violations	Number of unauthorized access attempts to critical data	<5 per month[8]
Protection	Encryption Coverage	Percentage of critical data protected by encryption	>98%[8]
Monitoring	Alert Response Time	Average time to respond to critical data alerts	<30 minutes[9]
Monitoring	False Positive Rate	Percentage of alerts that are false positives	<15%[9]
Training	Training Completion	Percentage of staff who completed required training	100%[10]

Source: [6] ISACA Data Governance Maturity Model (2023), [7] Grant Thornton's FINMA Implementation Benchmarks (2023), [8] NIST Cybersecurity Framework metrics for financial services (2023), [9] SANS Institute Financial Services Security Metrics (2024), [10] FINMA standard requirement for regulatory compliance training

Conclusion

FINMA Circular 2023/1 represents a significant evolution in regulatory expectations for operational resilience in the Swiss financial sector, with critical data risk management emerging as a cornerstone requirement. The June 1, 2024 compliance deadline creates urgency for institutions to implement comprehensive frameworks that address all aspects of critical data governance, protection, and monitoring.

Organizations that approach this challenge strategically, rather than as a mere compliance exercise, will realize substantial benefits beyond regulatory compliance. Enhanced operational resilience, improved data governance, reduced operational losses, and strengthened customer trust are among the potential advantages of a robust critical data risk management capability.

The implementation journey requires commitment from all levels of the organization, from the executive board to operational staff. Clear governance structures, comprehensive policies and procedures, and appropriate technical controls must be integrated into a cohesive approach that is proportionate to the institution's size, complexity, and risk profile.

As the financial industry continues its digital transformation journey, the importance of critical data will only increase. FINMA Circular 2023/1 provides a framework for establishing the capabilities needed to protect this essential asset, not just for regulatory compliance, but as a foundation for future business success.

Financial institutions should act now to assess their current capabilities, develop implementation roadmaps, and allocate the necessary resources to meet the regulatory deadline while positioning themselves for long-term operational resilience in an increasingly data-dependent industry.

References

- FINMA Circular 2023/1 "Operational Risks and Resilience - Banks" (December 2022)
- Basel Committee on Banking Supervision, "Principles for Operational Resilience" (March 2021)
- International Organization for Standardization, "ISO/IEC 27001:2022 - Information Security Management Systems" (2022)
- Swiss Data Protection Act (revised version, September 2023)
- Financial Stability Board, "Effective Practices for Cyber Incident Response and Recovery" (October 2020)
- European Banking Authority, "Guidelines on ICT and Security Risk Management" (EBA/GL/2019/04)
- National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity" (Version 1.1, 2018)
- [1] Deloitte Switzerland, "Financial Services Implementation Study: FINMA Circular 2023/1 Cost Impact Analysis" (2023)
- [2] PwC Switzerland, "Banking Compliance Cost Analysis: Operational Resilience Implementation" (2023)
- [3] IBM Security, "Cost of a Data Breach Report 2024" (January 2024)
- [4] Ponemon Institute, "Cost of Compliance Study: Financial Services Edition" (2023)
- [5] EY, "Financial Services Regulatory Technology Survey: Switzerland Focus" (2023)