SILVERFORT

MAS

White Paper

MAS Technology Risk Management Guidelines Compliance with Silverfort Unified Identity Protection

Table of Contents

Foreword

This document contains a detailed explanation of how the Silverfort Unified Identity Protection platform can assist you in complying with the MAS Technology Risk Management Guidelines. Silverfort addresses all of the guidelines' identity protection requirements, enhancing your overall security posture and increasing your resilience to various attack scenarios.

MAS Technology Risk Management Guidelines

On January 18, 2021, the Monetary Authority of Singapore (MAS) released a revised version of the Technology Risk Management (TRM) Guidelines, with the purpose of providing Financial Institutes (FI) with a comprehensive framework to assist in the forming of a sound cybersecurity strategy.

The MAS guidelines comprise a set of technology risk management principles and best practices that apply to all FIs that fall under MAS regulation, ranging from large ones like banks, insurance companies and exchanges to small ones like venture capital managers and payment services firms.

MAS Guidelines: The Identity Protection Aspect

A closer look at today's threat landscape reveals an increasing trend of identity-based attacks that utilize compromised credentials for malicious access to resources. These attacks occur both as a standalone malicious act such as account takeovers as well as a key component in larger scale operations such as lateral movement and ransomware propagation. In both cases the business risk these identity-based attacks introduce is critical.

Acknowledging this risk, the MAS guidelines include not only a dedicated Access Control section that explicitly deals with user access management, privileged access management and remote access management, but also multiple identity-related references in the context of cyber resilience, incident response and auditing. Complying with all these identity-related principles and practices would materially increase the FI's overall resilience to cyberattacks.

Silverfort Unified Identity Protection

The Silverfort Unified Identity Protection platform enables FI to comply with all the Identity Protection aspects of the MAS guidelines across the following sections:

- **Section 4: Technology Risk Management Framework**
- **Section 9: Access Control**
- **Section 11: Data and Infrastructure Security**
- **Section 12: Cyber Security Operations**
- **Section 15: IT Audit**

Zooming in: Two levels of Silverfort support

- **Section 9: Access Control**

  Silverfort provides complete coverage to the Access Control section with its innovative agentless and proxyless MFA solution that extends MFA protection to resources that could never have been protected before in that manner – endpoints, servers, IT infrastructure and others. In the context of FI one should especially note non-web applications that play a key role in banks but do not natively support MFA solutions. Silverfort secures this type of resource as well.

- **Sections 4, 11,12, 15**

  Here Silverfort supports various identity aspects of these sections. For example, in the section that deals with assessing risk, Silverfort contributes by providing real-time risk scoring for all authentications and access attempts. In the section that deals with investigation, Silverfort contributes by providing detailed access logs to all on-prem and cloud resources, that otherwise would require manual effort to retrieve and correlate, and so on.

The Silverfort Unified Identity Protection platform is your ultimate companion to the identity protection part of your journey towards the full adoption and implementation of MAS guidelines. The next chapter provides a detailed breakdown of the principles and practices that Silverfort supports.

Silverfort Unified Identity Protection - MAS Guidelines Compliance Breakdown

How to Use these Tables

The following tables include all the principals, practices in MAS guidelines that are related to identity protection and the respective Silverfort functionalities that address them. There is a separate table for each MAS Guidelines section.

Silverfort MAS Guidelines Compliance Tables

Table 1: MAS Guidelines Section 4: Technology Risk Management Framework

	MAS Technology Risk Management Guidelines	Silverfort Unified Identity Protection
4.1	Risk Management Framework	The Silverfort platform supports the Identity Protection aspects of the technology risk management guidelines as detailed in the following sections.
4.2	Risk Identification	Activity Monitoring and Risk Analysis
4.2.1	The FI should identify the threats and vulnerabilities applicable to its IT environment, including information assets that are maintained or supported by third party service providers. Examples of security threats that could have a severe impact on the FI and its stakeholders include internal sabotage, malware and data theft.	The Silverfort platform delivers continuous monitoring and risk analysis for every on-prem and cloud authentications and access attempts.
4.3	Risk Assessment	Risk Scoring

4.3.1	The FI should perform an analysis of the potential impact and consequences of the threats and vulnerabilities on the overall business and operations. The FI should take into consideration financial, operational, legal, reputational and regulatory factors in assessing technology risks.	The Silverfort platform rates the risks it detects as either low, medium, high, or critical. These risk scores apply to user accounts (human users and service accounts), on-prem and cloud resources and the authentication process itself.
4.3.2	To facilitate the prioritisation of technology risks, a set of criteria measuring and determining the likelihood and impact of the risk scenarios should be established.	
4.4	Risk Treatment	Proactive Access Policies
4.4.1	The FI should develop and implement risk mitigation and control measures that are consistent with the criticality of the information assets and the level of risk tolerance. The IT control and risk mitigation approach should be subject to regular review and update, taking into account the changing threat landscape and variations in the FI's risk profile.	The Silverfort platform enforces proactive access policies on all users accessing any resource to prevent threat actors from performing malicious access.
4.4.2	As there are residual risks from threats and vulnerabilities which cannot be fully eliminated, the FI should assess whether risks have been reduced to an acceptable level after applying the mitigating measures. The criteria and approving authorities for risk acceptance should be clearly defined and it should be commensurate with the FI's risk tolerance.	The Silverfort platform risk scoring is instrumental in assessing whether the environment is still at risk, as any malicious presence and activity is immediately captured and reflected in the various entities' risk scores.
4.5	Risk Monitoring, Review and Reporting	Risk Insights Dashboard

4.5.1	The FI should institute a process for assessing and monitoring the design and operating effectiveness of IT controls against identified risks.	The Silverfort platform provides a risk insights dashboard to accommodate granular real time visibility into all the components that comprise the protected environment's overall risk posture.
4.5.2	A risk register should be maintained to facilitate the monitoring and reporting of technology risks. Significant risks should be monitored closely and reported to the board of directors and senior management. The frequency of monitoring and reporting should be commensurate with the level of risk.	
4.5.3	To facilitate risk reporting to management, technology risk metrics should be developed to highlight information assets that have the highest risk exposure. In determining the technology risk metrics, the FI should take into account risk events and audit observations, as well as applicable regulatory requirements.	

Table 2: MAS Guidelines Section 9: Access Control

	MAS Technology Risk Management Guidelines	Silverfort Unified Identity Protection
9.1	User Access Management	Identity Zero Trust
9.1.1	The principles of 'never alone', 'segregation of duties', and 'least privilege' should be applied when granting staff access to information assets so that no one person has access to perform sensitive system functions. Access rights and system privileges should be granted according to the roles and responsibilities of the staff, contractors and service providers.	The Silverfort platform enables fulfilment of the listed principles through implementation of comprehensive Zero Trust access polices across the FI's on-prem and cloud resources.

9.1.2	The FI should establish a user access management process to provision, change and revoke access rights to information assets. Access rights should be authorised and approved by appropriate parties, such as the information asset owner.	The Silverfort platform prevents threat actors' malicious access attempts with adaptive access policies that either step-up authentication requirements with MFA or block access altogether.
9.1.3	For proper accountability, the FI should ensure records of user access and user management activities are uniquely identified and logged for audit and investigation purposes. inappropriate access rights. Exceptions noted from the user access review should be resolved as soon as practicable.	The Silverfort platform generates detailed logs of all users' access attempts, providing the full access trail of every user account to all on-prem and cloud resources.
9.1.4	The FI should establish a password policy and a process to enforce strong password controls for users' access to IT systems.	The Silverfort platform monitors the frequency of password changes, enabling the FI to detect stale passwords.
9.1.5	Multi-factor authentication should be implemented for users with access to sensitive system functions to safeguard the systems and data from unauthorised access.	The Silverfort platform enables the enforcement of MFA access polices across any on-prem or cloud resource. Silverfort is the only solution that can enforce MFA protection on command line access tools (PsExec, PowerShell, etc.) to workstations and servers, as well as to business non-web applications.
9.1.6	The FI should ensure appropriate parties such as information asset owners perform periodic user access review to verify the appropriateness of privileges that are granted to users. The user access review should be used to identify dormant and redundant user accounts, as well as inappropriate access rights. Exceptions noted from the user access review should be resolved as soon as practicable.	The Silverfort platform provides visibility into all stale accounts and admin users to assist in revealing any redundant users with high privileges.

9.1.7	Users should only be granted access rights on a need-to-use basis. Access rights that are no longer needed, as a result of a change in a user's job responsibilities or employment status (e.g. transfer or termination of employment), should be revoked or disabled promptly.	The Silverfort platform enables the FI to detect 'ghost admins', that is to say, users that maintained former high access privileges despite being transferred from an administrative position.
9.1.8	The FI should subject its service providers, who are given access to the FI's information assets, to the same monitoring and access restrictions on the FI's personnel.	The Silverfort platform enforces its adaptive access controls on service providers in the same manner it does for the FI employees.
9.2	Privileged Access Management	Access Policies for Privileged Accounts
9.2.1	Users granted privileged system access have the ability to inflict severe damage on the stability and security of the FI's IT environment. Access to privileged accounts should only be granted on a need-to-use basis; activities of these accounts should be logged and reviewed as part of the FI's ongoing monitoring.	The Silverfort platform enforces both rule based and adaptive risk based access policies to ensure that the privileged account is not compromised. The Silverfort platform logs the activity of all user accounts, including highly privileged ones.
9.2.2	System and service accounts are used by operating systems, applications and databasesto interact or access other systems' resources. The FI should establish a process to manage and monitor the use of system and service accounts for suspicious or unauthorised activities.	The Silverfort platform provides automated discovery, monitoring and risk analysis for all the service accounts in the protected environment. In addition, the Silverfort platform autonomously crafts a dedicated access policy for each service account based on its unique behavior, optionally blocking access for the account when an anomalous access request is detected.
9.3	Remote Access Management	Access Policies for Remote Connections

9.3.1	Remote access allows users to connect to the FI's internal network via an external network to access the FI's data and systems, such as emails and business applications. Remote connections should be encrypted to prevent data leakage through network sniffing and eavesdropping. Strong authentication, such as multi-factor authentication, should be implemented for users performing remote access to safeguard against unauthorised access to the FI's IT environment.	The Silverfort platform enforces adaptive access policies on remote connections to either step-up authentication with MFA or block access altogether when detecting a risk.

Table 3: MAS Guidelines Section 11: Data and Infrastructure Security

	MAS Technology Risk Management Guidelines	Silverfort Unified Identity Protection
11.1	Data Security	Threat Detection and Prevention
11.1.2	The FI should implement appropriate measures to prevent and detect data theft, as well as unauthorised modification in systems and endpoint devices. The FI should ensure systems managed by the FI's service providers are accorded the same level of protection and subject to the same security standards.	The Silverfort platform continuously monitors risk of users and machines to detect and proactively prevent threat actors' access to resources that contain sensitive data.
11.1.3	Systems and endpoint devices are often targeted by cyber criminals to gain access or exfiltrate confidential data within an organisation. As such, confidential data stored in systems	
11.1.5	Security measures should be implemented to prevent and detect the use of unauthorised internet services which allow users to communicate or store confidential data. Examples of such services include social media, cloud storage and file sharing, emails, and messaging applications.	The Silverfort platform enforces MFA protection on various remote connections, including file shares, email service and others.

11.2	Network Security	Lateral Movement Protection
11.2.2	To minimise the risk of cyber threats, such as lateral movement and insider threat, the FI should deploy effective security mechanisms to protect information assets. Information assets could be grouped into network segments based on the criticality of systems, the system's functional role (e.g. database and application) or the sensitivity of the data.	The Silverfort platform enforces MFA access policies on all access interfaces in Active Directory environments including RDP and command line access tools such as PsExc, Remote Powershell and others. Using MFA to secure these access interfaces proactively prevents most to all of lateral movement attacks.
11.3	System Security	Continuous Risk Monitoring
11.3.1	The security standards for the FI's hardware and software (e.g. operating systems, databases, network devices and endpoint devices) should outline the configurations that will minimise their exposure to cyber threats. The standards should be reviewed periodically for relevance and effectiveness	The Silverfort platform includes an additional free tool that scans systems for identity-related vulnerabilities.
11.3.5	To facilitate early detection and prompt remediation of suspicious or malicious systems activities, the FI should implement detection and response mechanisms to perform scanning of indicators of compromise (IOCs) in a timely manner, and proactively monitor systems', including endpoint systems', processes for anomalies and suspicious activities.	The Silverfort platform provides a detailed investigation dashboard to facilitate both forensic investigations as well as proactive threat hunting across the protected environment.
11.4	Virtualisation Security	Access Policies for Virtualization Administration

11.4.1	Virtualisation 24 is used by organisations to optimise the use of computing resources and to enhance resilience. The technology allows several virtual machines (VMs) that support different business applications to be hosted on a physical system. A system failure or security breach in one of the VMs could have contagion impact on other VMs. The FI should ensure security standards are established for all components of a virtualisation solution.	The Silverfort platform secures the admin access to the virtualization platform with adaptive policies that either step-up authentication with MFA or block access altogether when risk is detected.

Table 4: MAS Guidelines Section 12: Cyber Security Operations

	MAS Technology Risk Management Guidelines	Silverfort Unified Identity Protection
12.2	Cyber Event Monitoring and Detection	Continuous Risk Monitoring
12.2.1	To facilitate continuous monitoring and analysis of cyber events; as well as prompt detection and response to cyber incidents, the FI should establish a security operations centre or acquire managed security services. The processes, roles and responsibilities for security operations should be defined.	The Silverfort platform continuously monitors and evaluates the risk of all identity-related activities (authentications and access attempts) and entities (user accounts, machines and applications).
12.2.2	A process to collect, process, review and retain system logs should be established to facilitate the FI's security monitoring operations. These logs should be protected against unauthorised access.	The Silverfort platform provides detailed logs on every authentication and access attempt.

12.2.3	To facilitate identification of anomalies, the FI should establish a baseline profile of each IT system's routine activities and analyse the system activities against the baseline profiles. The profiles should be regularly reviewed and updated. anomalous behaviours.	The Silverfort platform creates a real time behavioral baseline for each user account. Anomalous behavior increases the user account's risk score that is both forwarded to 3rd party security products (SIEM, Log Analytics, SOAR, etc.) and triggers Silverfort's adaptive access policies.
12.2.5	Correlation of multiple events registered on system logs should be performed to identify suspicious or anomalous system activity patterns.	The Silverfort platform makes available all authentication and access attempts logs for correlation and detection of suspicious behavior.
12.2.6	A process should be established to ensure timely escalation to relevant stakeholders regarding suspicious or anomalous system activities or user behaviour.	The Silverfort platform monitors dozens of risk indicators that indicate malicious presence or activity. Each risk indicator can be set as a trigger to an access policy that would either step-up authentication with MFA or block access altogether. In both cases escalation to the response team occurs in real time.
12.3	Cyber Incident Response and Management	Attack Detection and Prevention
12.3.1	The FI should establish a cyber incident response and management plan to swiftly isolate and neutralise a cyber threat and to securely resume affected services. The plan should describe communication, coordination and response procedures to address plausible cyber threat scenarios.	The Silverfort platform responds to detected threats with real time access prevention (MFA or block). This effectively neutralizes the attacker's ability to access the resources while providing the security team the required data to locate and remediate the entailed compromised user accounts and machines.
12.3.2	As part of the plan, the FI should establish a process to investigate and identify the security or control deficiencies that resulted in the security breach. The investigation should also evaluate the full extent of the impact to the FI.	The Silverfort platform provides all the identity-related forensic data to investigate a breach.

12.3.3	Information from cyber intelligence and lessons learnt from cyber incidents should be used to enhance the existing controls or improve the cyber incident management plan.	The Silverfort platform access policies can be fine-tuned and enhanced based on lessons learned from previous incidents.

Table 5: MAS Guidelines Section 15: IT Audit

	MAS Technology Risk Management Guidelines	Silverfort Unified Identity Protection
15.1	Audit Function	Inventory Management
15.1.1	Audit plays an important role to assess the effectiveness of the controls, risk management and governance process in the FI. The FI should ensure IT audit is performed to provide the board of directors and senior management an independent and objective opinion of the adequacy and effectiveness of the FI's risk management, governance and internal controls relative to its existing and emerging technology risks.	The Silverfort platform provides a full inventory list of all user accounts, machines and applications within the protected environment, facilitating a rapid and seamless auditing process for these entities.
15.1.2	A comprehensive set of auditable areas for technology risk should be identified so that an effective risk assessment could be performed during audit planning. Auditable areas should include all IT operations, functions and processes.	
15.1.3	The frequency of IT audits should be commensurate with the criticality of and risk posed by the IT information asset, function or process.	
15.1.4	The FI should ensure its IT auditors have the requisite level of competency and skills to effectively assess and evaluate the adequacy of IT policies, procedures, processes and controls implemented.	

About Silverfort

Silverfort has pioneered the first-ever Unified Identity Protection platform, which protects enterprises against identity-based attacks that utilize compromised credentials to access enterprise resources. Using innovative agentless and proxyless technology, Silverfort natively integrates with all existing IAM solutions, to extend secure access controls such as Risk-Based Authentication and MFA across all on-prem and cloud resources. This includes assets that could never have been protected in this way before, such as homegrown/legacy applications, IT infrastructure, file systems, command-line tools, machine-to-machine access, and more. Silverfort continuously monitors all access attempts by users and service accounts, and analyzes risks in real-time using an AI-based engine to enforce adaptive access policies.

To learn more, visit www.silverfort.com

info@silverfort.com

www.Silverfort.com

US
(+1) 646 893 7857
43 Westland Avenue,
Boston, MA, USA

Israel
(+972) 77 202 4900
30 Haarbaa St, 26th Floor,
Tel Aviv, Israel