SOLUTION GUIDE

How StrongDM Helps with the Cloud Control Matrix (CCM) 4.0

The Cloud Controls Matrix (CCM) is developed by the Cloud Security Alliance (CSA). This framework is designed to aid both cloud providers and consumers in evaluating the security posture of cloud services. It comprises a collection of widely recognized security controls and best practices to provide organizations with guidance to effectively manage security risks in the cloud.

Below are the specific requirements where StrongDM can help you meet CCM 4.0 for the Identity & Access Management requirements. We have also provided a subset of the control mappings as a reference.

Control Domain: Identity & Access Management	
Control ID & Name	IAM-05 Least Privilege
Control Specification	Employ the least privilege principle when implementing information system access.
StrongDM Capability	Grant temporary or Just-in-Time access, with least privilege by default, for managing access to critical infrastructure. Integrate testing, approving, and implementing changes necessary in emergency situations (e.g. grant temporary access within applications like Slack and Microsoft Teams).
Control Mapping	**AICPA TSC 2017**: CC6.3 **CIS 8.0**: 6.8 **ISF SOGP 2022**: SAI.1 **ISO/IEC 27001/27002 2022**: 27001: A.5.15 27001: A.8.2 27002:5.15 **NIST 800-53 5**: AC-6 AC-6(4) IA-12 IA-12(2) IA-12(3) **NIST CSF 1.1**: PR.AC-4 **PCI DSS 4.0**: 7.2.1 7.2.2 7.2.5 7.2.6

Control Domain: Identity & Access Management

Control ID & Name	IAM-06 **User Access Provisioning**
Control Specification	Define and implement a user access provisioning process which authorizes, records, and communicates access changes to data and assets.
StrongDM Capability	StrongDM is a Dynamic Access Management platform that centralizes privileged access for all technical users to every resource in your infrastructure, on-premises and in the cloud. Every activity and query is logged for complete visibility into who is accessing what, when, and how. End users connect through StrongDM without ever being expsoed to credentials.
Control Mapping	**AICPA TSC 2017**: CC6.3 CC8.1 **CIS 8.0**: 6.1 **ISF SOGP 2022**: SAI.1.3 **ISO/IEC 27001/27002 2022**: 27001: A.5.15 27002: 5.16 27002: 5.18 **NIST 800-53 5**: AC-3 AC-16 AC-16(2) AC-16(4) AC-16(10) IA-12 IA-12(1) **NIST CSF 1.1**: PR.AC-1 PR.PT-1 PR.AC-4 **PCI DSS 4.0**: 7.2.2 7.2.3 8.2.4

Control ID & Name	IAM-07 **User Access Changes and Revocation**
Control Specification	De-provision or respectively modify access of movers / leavers or system identity changes in a timely manner in order to effectively adopt and communicate identity and access management policies.
StrongDM Capability	Access to critical infrastructure aligns with the identity lifecyle, permissions occur only through StrongDM which authenticates the users through your identity provider or through StrongDM with MFA.
Control Mapping	**AICPA TSC 2017**: CC5.3 CC6.3 **CIS 8.0**: 5.3 6.2 **ISF SOGP 2022**: SAI.1.3 **ISO/IEC 27001/27002 2022**: 27001: A.5.15 27001: A.5.18 **NIST 800-53 5**: AC-2 AC-2(1) AC-2(2) AC-2(6) AC-2(8) AC-3 AC-3(8) AC-6 AC-6(7) AU-10 AU-10(4) AU-16 AU-16(1) CM-7 CM-7(1) **NIST CSF 1.1**: PR.AC-1 PR.AC-4 PR.IP-11 **PCI DSS 4.0**: 8.2.5 8.2.6

Control Domain: Identity & Access Management

Control ID & Name	IAM-08 **User Access Review**
Control Specification	Review and revalidate user access for least privilege and separation of duties with a frequency that is commensurate with organizational risk tolerance.
StrongDM Capability	The Standing Access Dashboard shows the secutity risk profile of all standing access grants. Make decisons on how should continue to have access, and where access can be revoked without introducing friction.
Control Mapping	**AICPA TSC 2017**: CC6.2 CC6.3 **CIS 8.0**: 5.1 **ISF SOGP 2022**: SAI.1.3 **ISO/IEC 27001/27002 2022**: 27001: A.5.3 27001: A.5.18 27001: A.8.3 **NIST 800-53 5**: AC-6 AC-6(4) AC-6(8) IA-8 IA-8(4) **NIST CSF 1.1**: PR.AC-4 **PCI DSS 4.0**: 7.2.5.1 7.2.5 7.2.4

Control ID & Name	IAM-09 **Segregation of Privileged Access Roles**
Control Specification	Define, implement and evaluate processes, procedures and technical measures for the segregation of privileged access roles such that administrative access to data, encryption and key management capabilities and logging capabilities are distinct and separated.
StrongDM Capability	The StrongDM Admin UI maintains a list of all users and resources they have access to. Admins can define and enforce the appropriate access policies based on a user's role or a resource's attributes with comprehensive permissions auditing available.
Control Mapping	**AICPA TSC 2017**: CC5.1 CC6.1 CC6.3 **CIS 8.0**: 5.4 **ISF SOGP 2022**: SAI.1.3 **ISO/IEC 27001/27002 2022**: 27001: A.8.2 27001: A.8.18 27002: 8.2 (j) **NIST 800-53 5**: AC-6 AC-3(7) AC-6(4) AC-6(8) IA-5 IA-5(6) IA-8 IA-8(4) **NIST CSF 1.1**: PR.AC-1 PR.AC-4 **PCI DSS 4.0**: 3.6.1 3.7.6 6.5.3 6.5.4 7.2.1 7.2.2 10.3.1

Control Domain: Identity & Access Management

Control ID & Name	IAM-10 Management of Privileged Access Roles
Control Specification	Define and implement an access process to ensure privileged access roles and rights are granted for a time limited period, and implement procedures to prevent the culmination of segregated privileged access.
StrongDM Capability	Grant temporary or Just-in-Time access, with least privilege by default, for managing access to critical infrastructure. Integrate testing, approving, and implementing changes necessary in emergency situations (e.g. grant temporary access within applications like Slack and Microsoft Teams).
Control Mapping	**AICPA TSC 2017**: CC6.1 CC6.2 CC6.3 **CIS 8.0**: 5.1 6.5 **ISF SOGP 2022**: SAI.1.3 **ISO/IEC 27001/27002 2022**: 27001: A.8.2 27001: A.8.18 27002: 8.2 (i) **NIST 800-53 5**: AC-2 AC-2(7) AC-3 AC-3(4) AC-3(11) AC-3(13) AC-3(14) AC-6 AC-6(4) AC-6(5) AC-6(8) AC-12 AC-12(3) AC-17 AC-17(4) IA-8 IA-8(4) **NIST CSF 1.1**: PR.AC-4 **PCI DSS 4.0**: 7.2.1 7.2.2

Control ID & Name	IAM-13 Uniquely Identifiable Users
Control Specification	Define, implement and evaluate processes, procedures and technical measures that ensure users are identifiable through unique IDs or which can associate individuals to the usage of user IDs.
StrongDM Capability	Access to critical infrastructure aligns with the identity lifecyle, permissions occur only through StrongDM which authenticates the users through your identity provider or through StrongDM with MFA.
Control Mapping	**AICPA TSC 2017**: CC6.1 **CIS 8.0**: No Mapping **ISF SOGP 2022**: SA1.3 **ISO/IEC 27001/27002 2022**: 27001: A.5.16 **NIST 800-53 5**: AC-3 AC-3(14) AC-24 AC-24(2) AU-10 AU-10(1) IA-2 IA-2(1) IA-2(12) IA-4 IA-4(1) SA-8 SA-8(22) SC-23 SC-23(3) SC-40(4) IA-2(2) **NIST CSF 1.1**: PR.AC-1 PR.AC-6 **PCI DSS 4.0**: 8.2.1 8.2.2 8.2.4

Control Domain: Identity & Access Management

Control ID & Name	IAM-16 **Authorization Mechanisms**
Control Specification	Define, implement and evaluate processes, procedures and technical measures to verify access to data and system functions is authorized.
StrongDM Capability	StrongDM's Access Workflows solution provides a comprehensive, auditable, and streamlined approach to managing user access rights and permissions through requests that grant access through automated or human approval.
Control Mapping	**AICPA TSC 2017**: CC6.1, CC6.2, CC6.3 **CIS 8.0**: 5.1 **ISF SOGP 2022**: SAI.1.3, SAI.1.4 **ISO/IEC 27001/27002 2022**: 27001: A.5.18 **NIST 800-53 5**: AC-3, AC-3(5), AC-4, AC-4(17), AC-4(21), AC-4(22), AC-6, AC-6(8), AC-6(9), AC-12, AC-12(1), AC-20, AC-20(1), AU-10, AU-10(1) **NIST CSF 1.1**: PR.AC-1, PR.AC-4, PR.AC-6, PR.AC-7, PR.PT-1 **PCI DSS 4.0**: 7.2.4, 7.2.3, 7.2.5.1