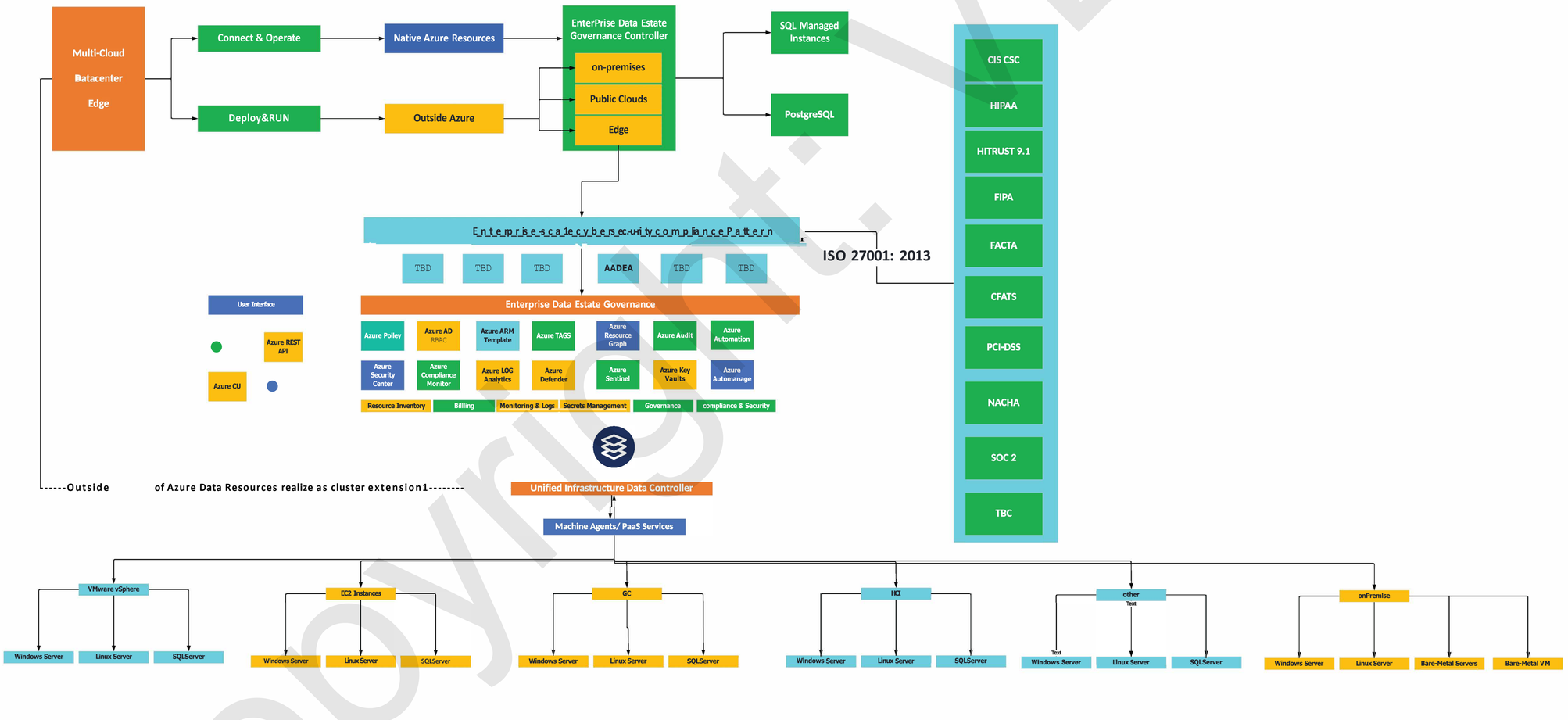
# Architectural Design Document (ADD) (Excerpt)

## Enterprise Cybersecurity Design Strategy

### Enterprise-Scale Cybersecurity Compliance Pattern

(C4 Level 1 diagram)




Draft v1.01
Dr. Olaf Cames
07/07/2022

Dr. Olaf Cames

Digitally signed by Dr. Olaf Cames
Date: 2022.12.29 21:57:03 -05'00'

copyright. YBIC

**Regulation:** SOC2
**Control ID:** PI1.3
**Control Family:** Additional Criteria For Processing Integrity
**Action:** Azure AD Entitlement Management (AADEA)
**Pattern:** 1002

# Regulation: SOC2

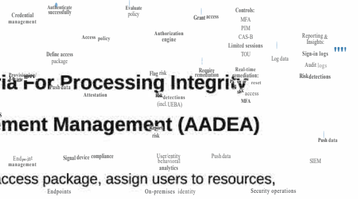
# Control ID: PI1.3

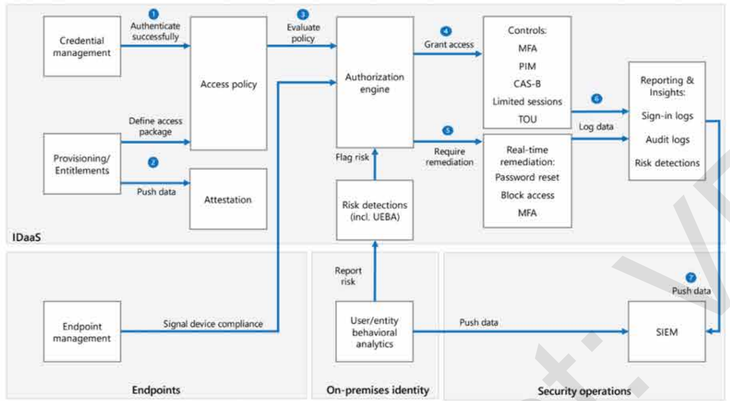
# Control Family: Additional Criteria For Processing Integrity

# Action: Azure AD Entitlement Management (AADEA)

# Pattern: 1002

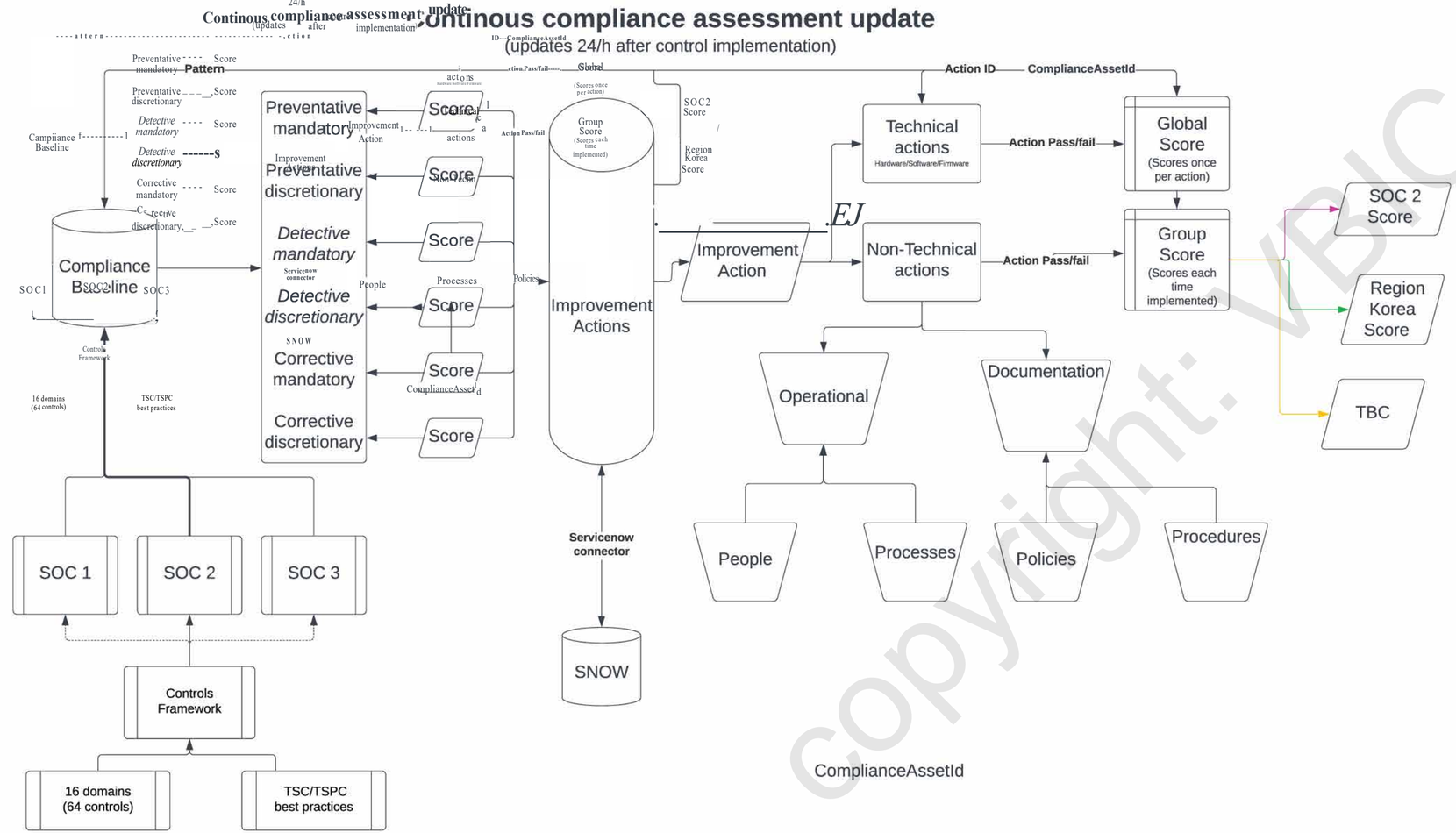
1. *Credential management* controls authentication.
2. *Provisioning* and *entitlement management* define the access package, assign users to resources, and push data for *attestation*.
3. The *authorization engine* evaluates the *access policy* to determine access. The engine also evaluates *risk detections*, including *user/entity behavioral analytics (UEBA)* data, and checks device compliance for *endpoint management*.
4. If authorized, the user or device gains access per *conditional access policies and controls*.
5. If authorization fails, users can do *real-time remediation* to unblock themselves.
6. All session data is *logged* for analysis and reporting.
7. The SOC team's *security information and event management system (SIEM)* receives all log, risk detection, and UEBA data from cloud and on-premises identities.




Draft v1.01
Dr. Olaf Cames
07/07/2022

copyright: VBIC




copyright: VBC

A

# Account Management - Identifying Account Types

Action ID: 1002

(D This action is managed by Microsoft and cannot be edited. learn more

**Overview**

Details

| | |
|---|---|
| Implementation Status | Test Status |
| Alternative Implementation | Passed |
| possible points | Managed by |
| 27 | Microsoft |
| Action scope | Action type |
| Global | Technical |
| Products | Documents |
| Azure | 0 |

Implementation | Testing | Standards and Regulations | Documents

Test status

- Passed

Test date

Sun Nov 14 2021

Testing notes

Procedure 1:Passed Determine if the organization:

- defines information system account types to be identified and selected to support organizational missions/business functions

Examine:
Access control policy; procedures addressing account management; security plan; information system design documentation; information system configu name of the individual associated with each account; list of conditions for group and role membership; notifications or records of recently transferred, ser

copyright: VBIC

A

# Account Management - Identifying Account Types

Action ID: 1002

CD This action is managed by Microsoft and cannot be edited. Learn more

**Overview**

Details

| | |
|---|---|
| Implementation Status<br>Alternative Implementation | Test Status<br>Passed |
| possible points<br>27 | Managed by<br>Microsoft |
| Action scope<br>Global | Action type<br>Technical |
| Products<br>Azure | Documents<br>0 |

Implementation Testing **Standards and Regulations** Documents

Filter Reset 7 . Filters

Regulation: **Any** v

| ) Control | Control ID | Control family | Regulation |
|---|---|---|---|
| **v SO(2 ()** | | | |
| System processing | PII.3 | Additional Criteria For Processing Integrity | SOC2 |

Copyright: VBRIC