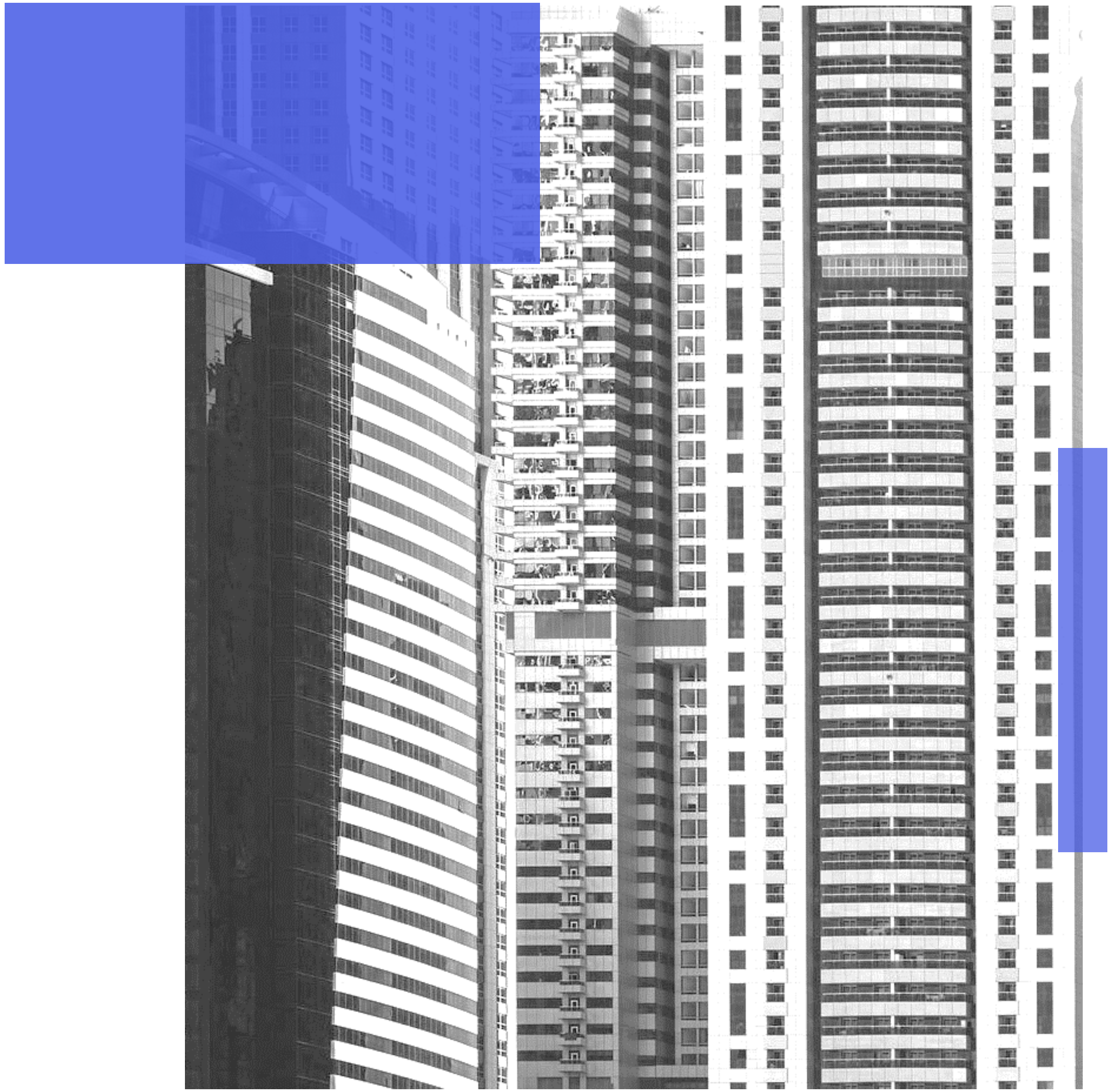
TONY SHEN

AZURE GOV CLOUD MIGRATION PLANNING



AGENDA

INTRODUCTION

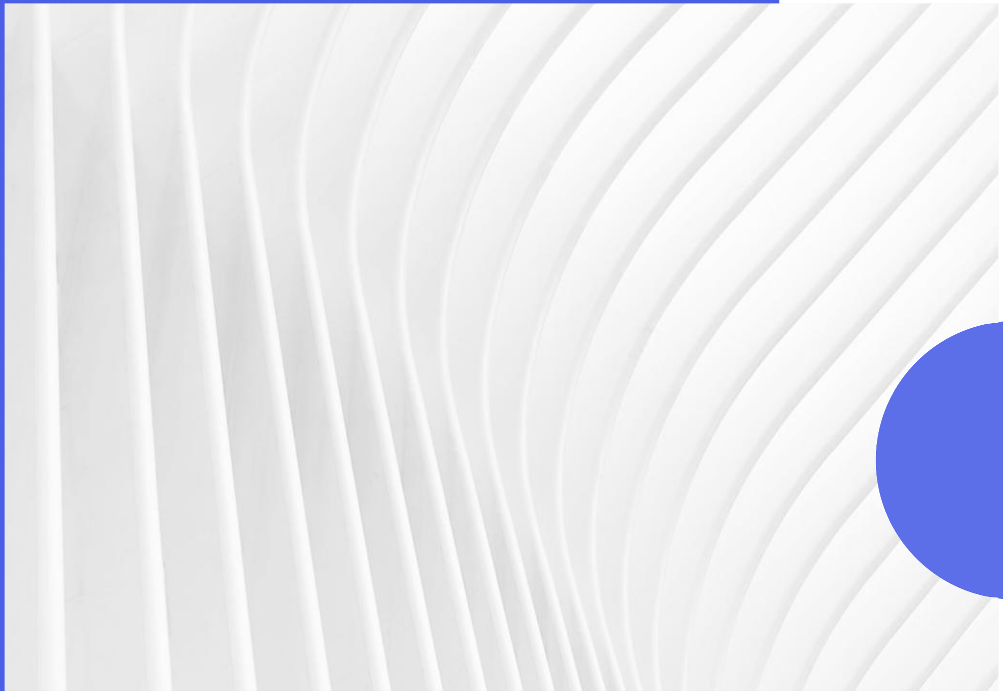
PRIMARY GOALS

PLANNING AND IMPLEMENTATION

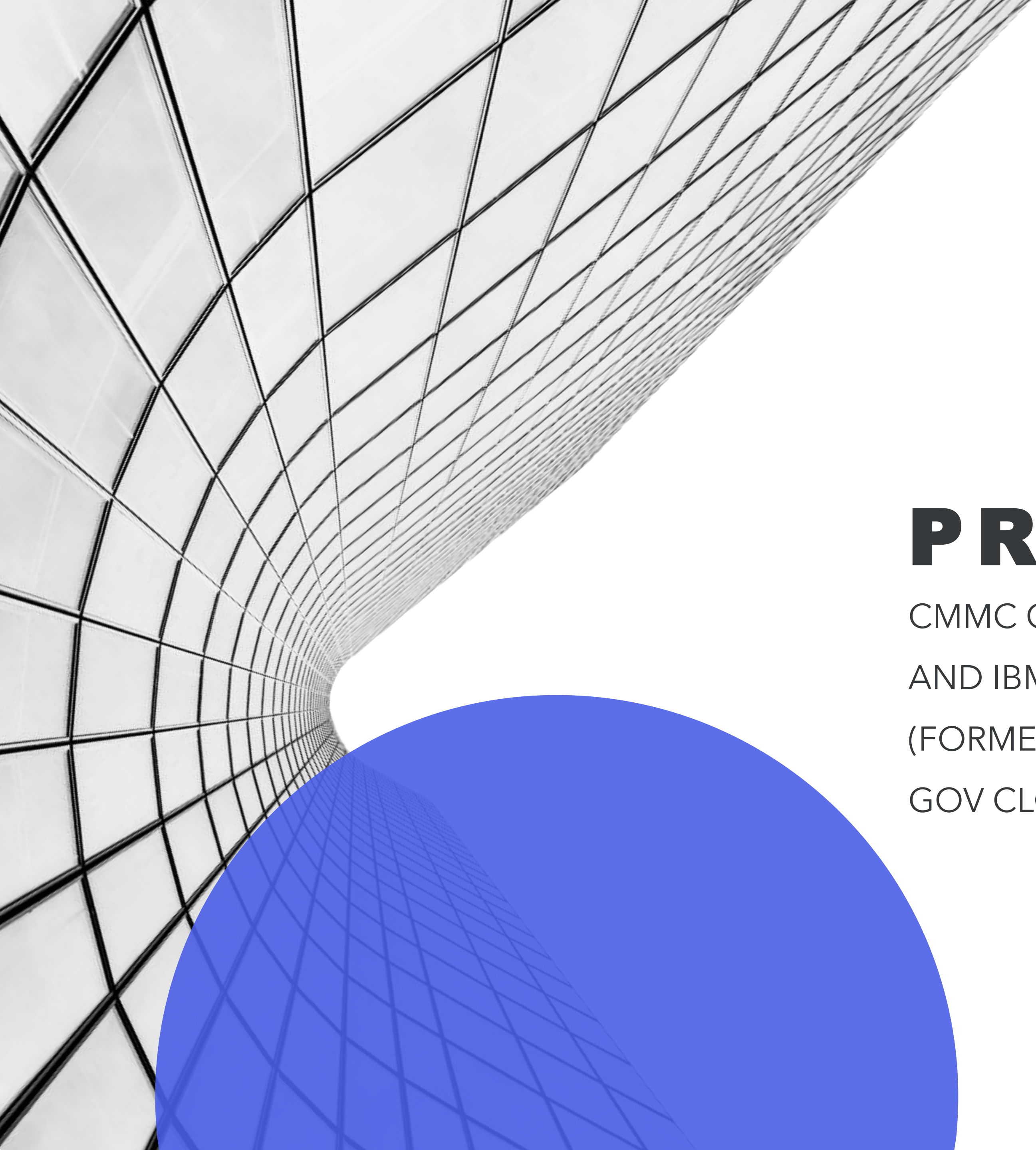
TIMELINE

SUMMARY

INTRO



At Tek Systems, we empower organizations to foster collaborative thinking to further drive workplace innovation. By closing the loop and leveraging agile frameworks, we help business grow organically and work with government hand in hand to make our country greater than it has ever been.



PRIMARY GOALS

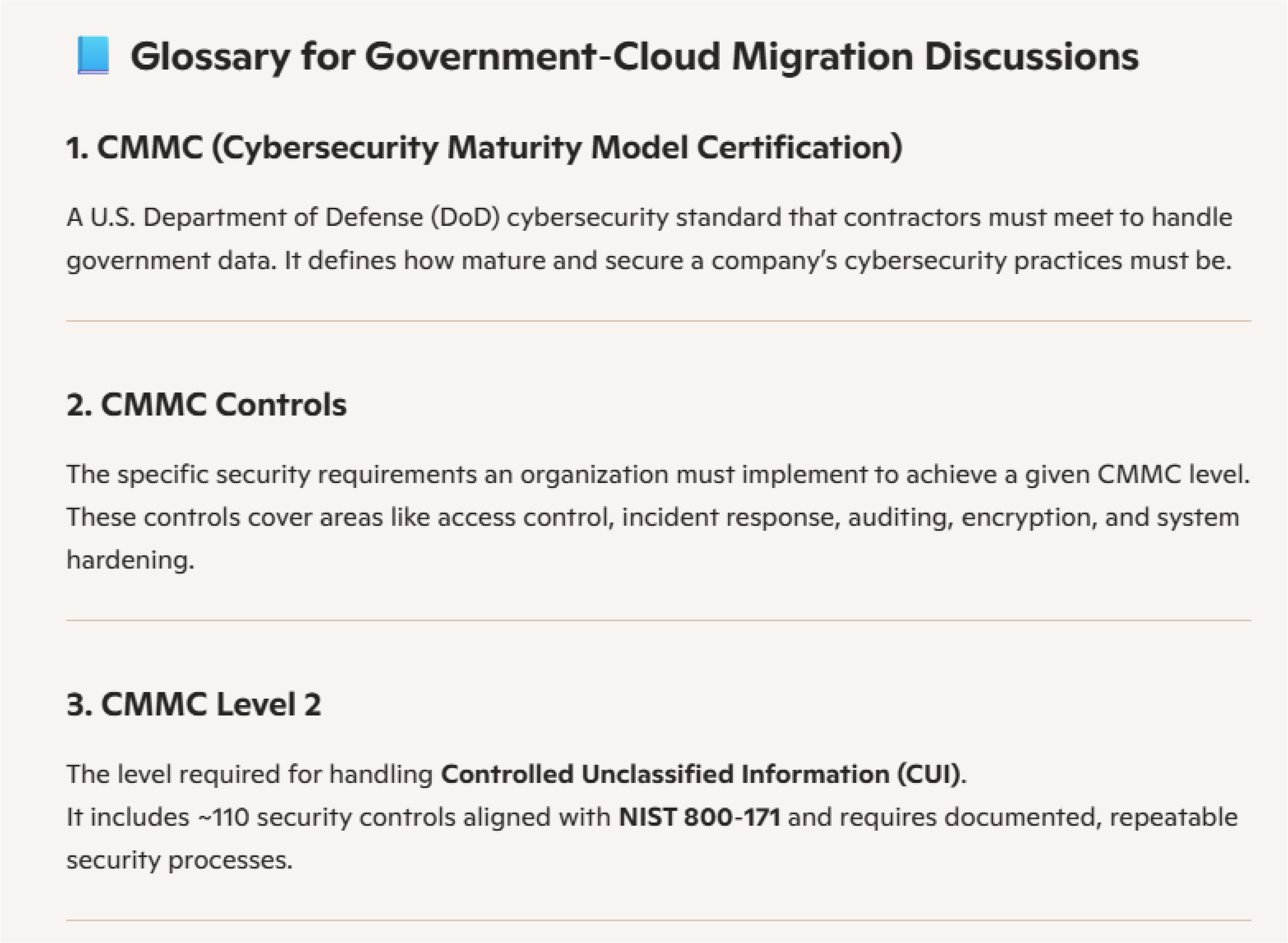
CMMC COMPLIANCE MIGRATION FROM LEGACY WINDCHILL AND IBM MAXIMO APPLICATIONS TO DEPARTMENT OF WAR (FORMERLY DEPARTMENT OF DEFENSE) MANDATED AZURE GOV CLOUD

PLANNING AND IMPLEMENTATION

2026	Assessment to complete	Readiness Gap Analyses to complete	Preparation to complete	Implementation to complete
Q1	100%	100%	50%	10%
Q2			100%	20%
Q3				50%
Q4				100%

PLANNING TOPICS

- Glossary for Azure Gov Cloud Migration Discussions
- Azure GCC High Migration Readiness Checklist
- Risk & Dependency Matrix for Windchill + Maximo Migration
- CMMC Level 2 Gap-Assessment
- Azure Gov Entra ID + Entra ID Governance to meet and exceed CMMC compliance in IAM



📘 Glossary for Government-Cloud Migration Discussions

1. CMMC (Cybersecurity Maturity Model Certification)

A U.S. Department of Defense (DoD) cybersecurity standard that contractors must meet to handle government data. It defines how mature and secure a company's cybersecurity practices must be.

---

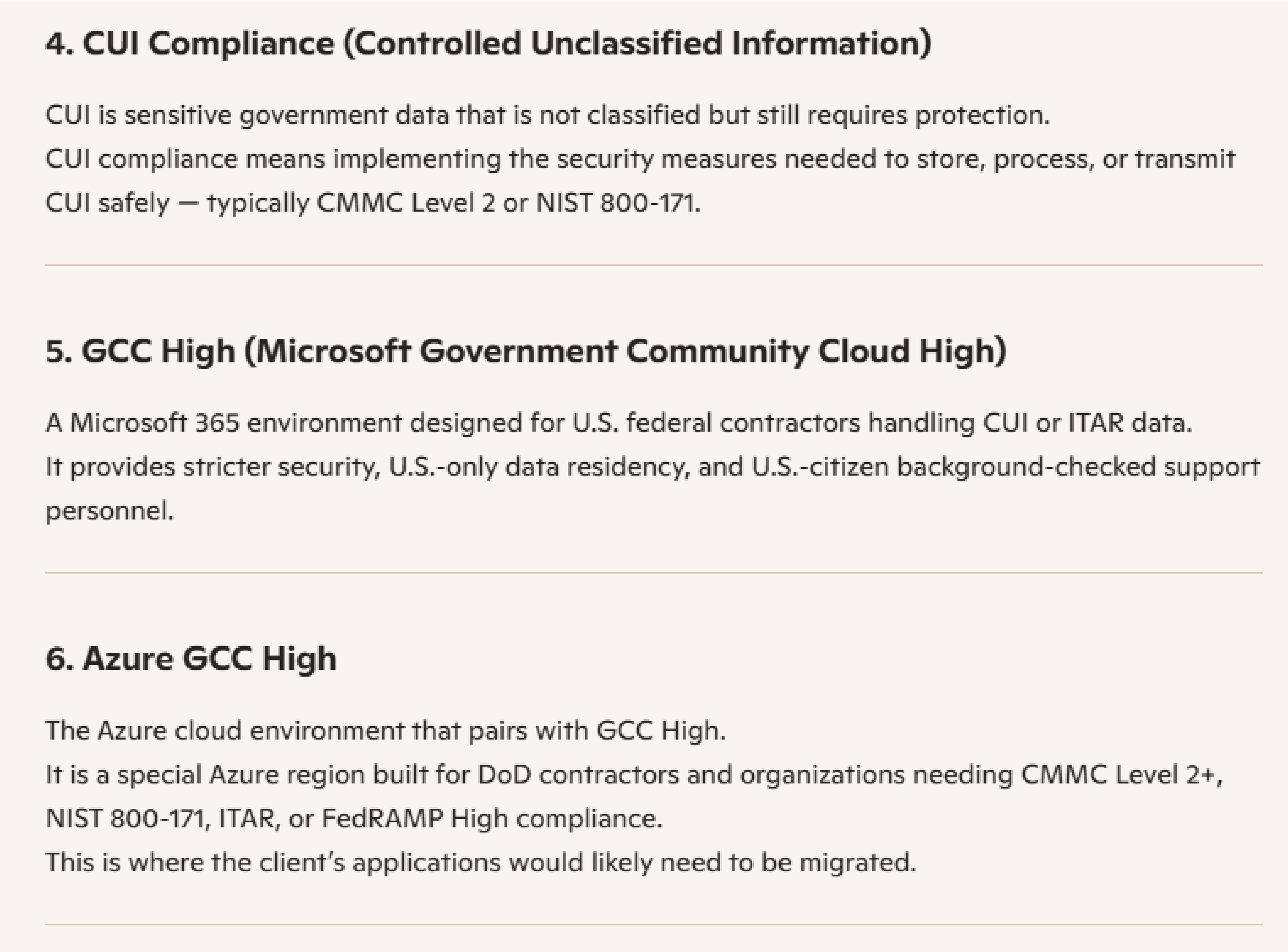
2. CMMC Controls

The specific security requirements an organization must implement to achieve a given CMMC level. These controls cover areas like access control, incident response, auditing, encryption, and system hardening.

---

3. CMMC Level 2

The level required for handling **Controlled Unclassified Information (CUI)**.
It includes ~110 security controls aligned with **NIST 800-171** and requires documented, repeatable security processes.



4. CUI Compliance (Controlled Unclassified Information)

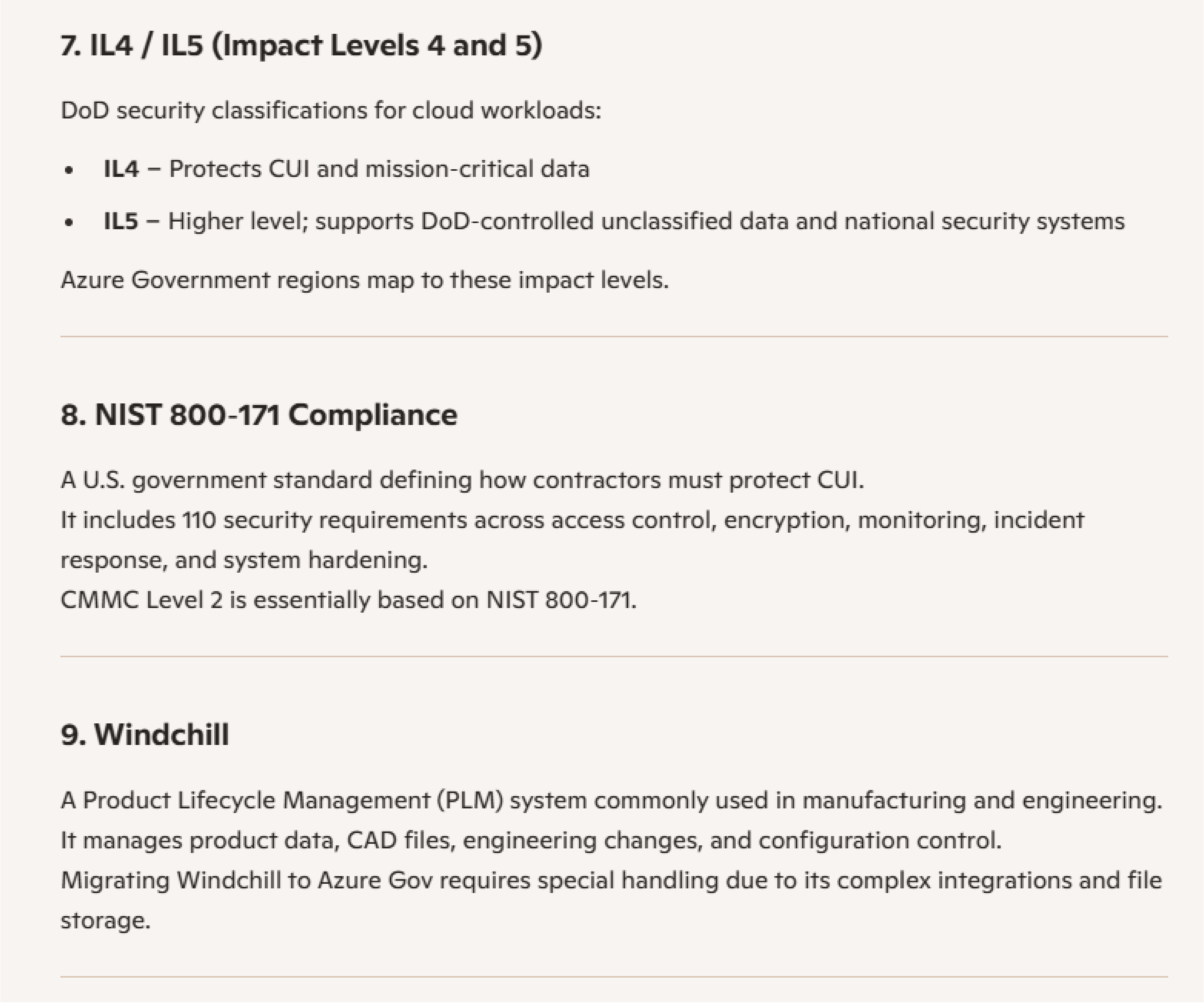
CUI is sensitive government data that is not classified but still requires protection.
CUI compliance means implementing the security measures needed to store, process, or transmit CUI safely — typically CMMC Level 2 or NIST 800-171.

5. GCC High (Microsoft Government Community Cloud High)

A Microsoft 365 environment designed for U.S. federal contractors handling CUI or ITAR data.
It provides stricter security, U.S.-only data residency, and U.S.-citizen background-checked support personnel.

6. Azure GCC High

The Azure cloud environment that pairs with GCC High.
It is a special Azure region built for DoD contractors and organizations needing CMMC Level 2+, NIST 800-171, ITAR, or FedRAMP High compliance.
This is where the client's applications would likely need to be migrated.



7. IL4 / IL5 (Impact Levels 4 and 5)

DoD security classifications for cloud workloads:

- **IL4** – Protects CUI and mission-critical data
- **IL5** – Higher level; supports DoD-controlled unclassified data and national security systems

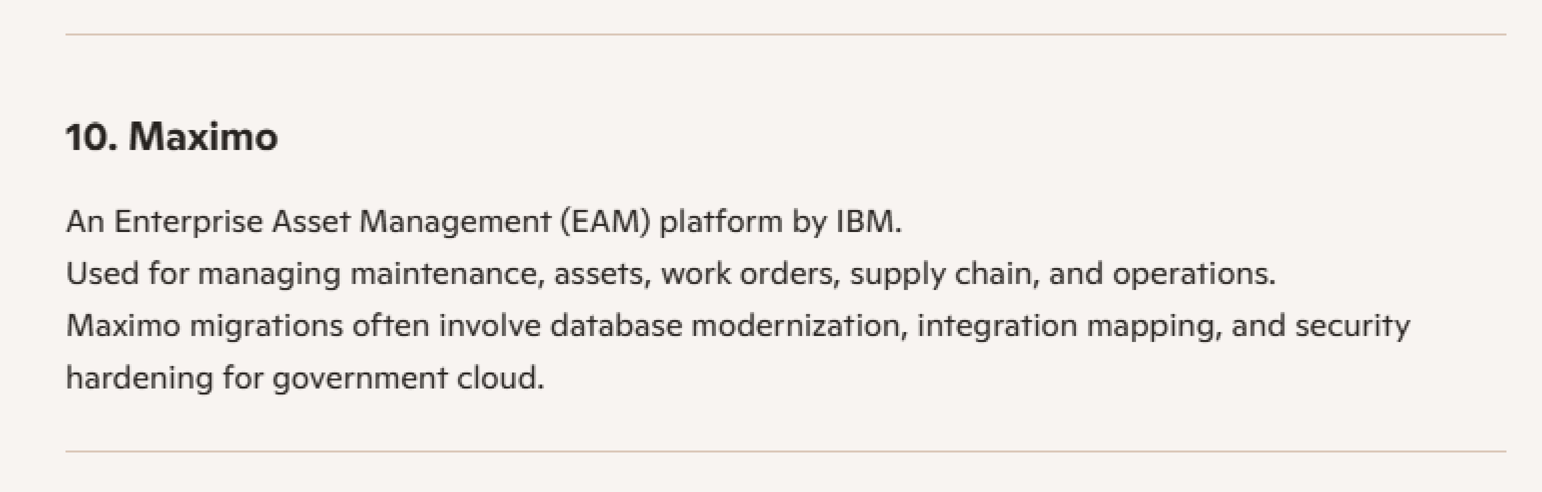
Azure Government regions map to these impact levels.

8. NIST 800-171 Compliance

A U.S. government standard defining how contractors must protect CUI.
It includes 110 security requirements across access control, encryption, monitoring, incident response, and system hardening.
CMMC Level 2 is essentially based on NIST 800-171.

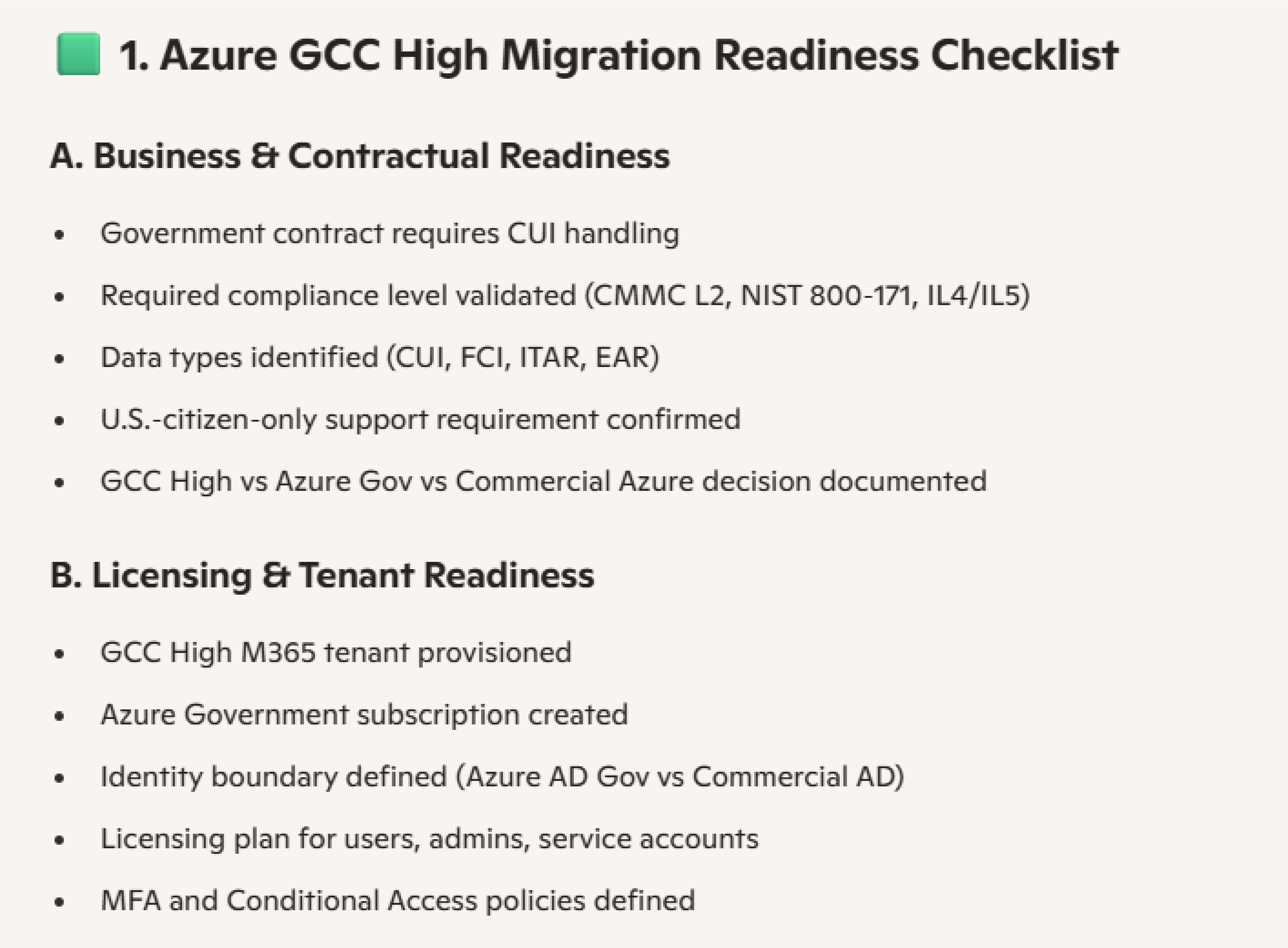
9. Windchill

A Product Lifecycle Management (PLM) system commonly used in manufacturing and engineering.
It manages product data, CAD files, engineering changes, and configuration control.
Migrating Windchill to Azure Gov requires special handling due to its complex integrations and file storage.



10. Maximo

An Enterprise Asset Management (EAM) platform by IBM.
Used for managing maintenance, assets, work orders, supply chain, and operations.
Maximo migrations often involve database modernization, integration mapping, and security hardening for government cloud.



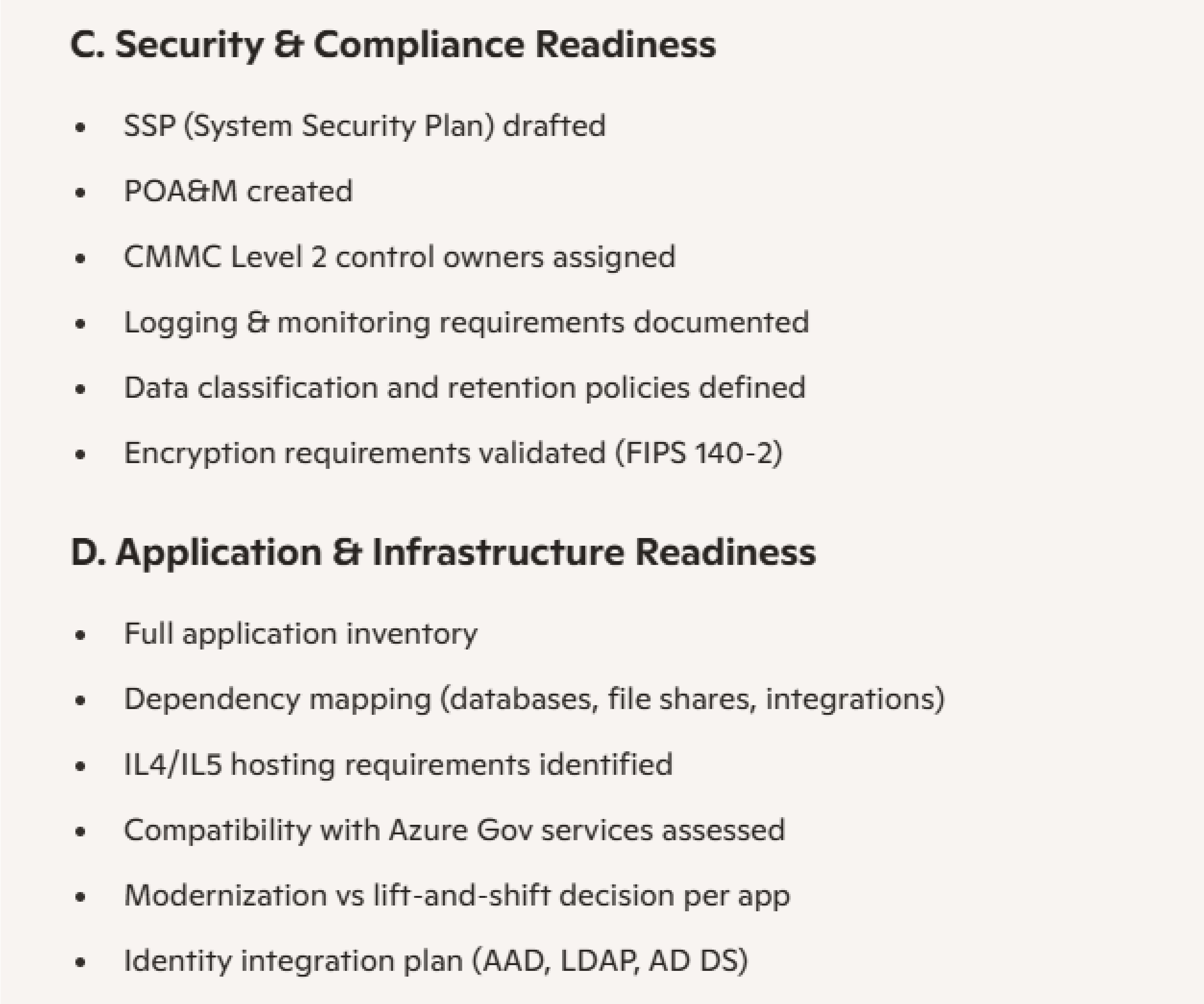
🟩 1. Azure GCC High Migration Readiness Checklist

A. Business & Contractual Readiness

- Government contract requires CUI handling
- Required compliance level validated (CMMC L2, NIST 800-171, IL4/IL5)
- Data types identified (CUI, FCI, ITAR, EAR)
- U.S.-citizen-only support requirement confirmed
- GCC High vs Azure Gov vs Commercial Azure decision documented

B. Licensing & Tenant Readiness

- GCC High M365 tenant provisioned
- Azure Government subscription created
- Identity boundary defined (Azure AD Gov vs Commercial AD)
- Licensing plan for users, admins, service accounts
- MFA and Conditional Access policies defined

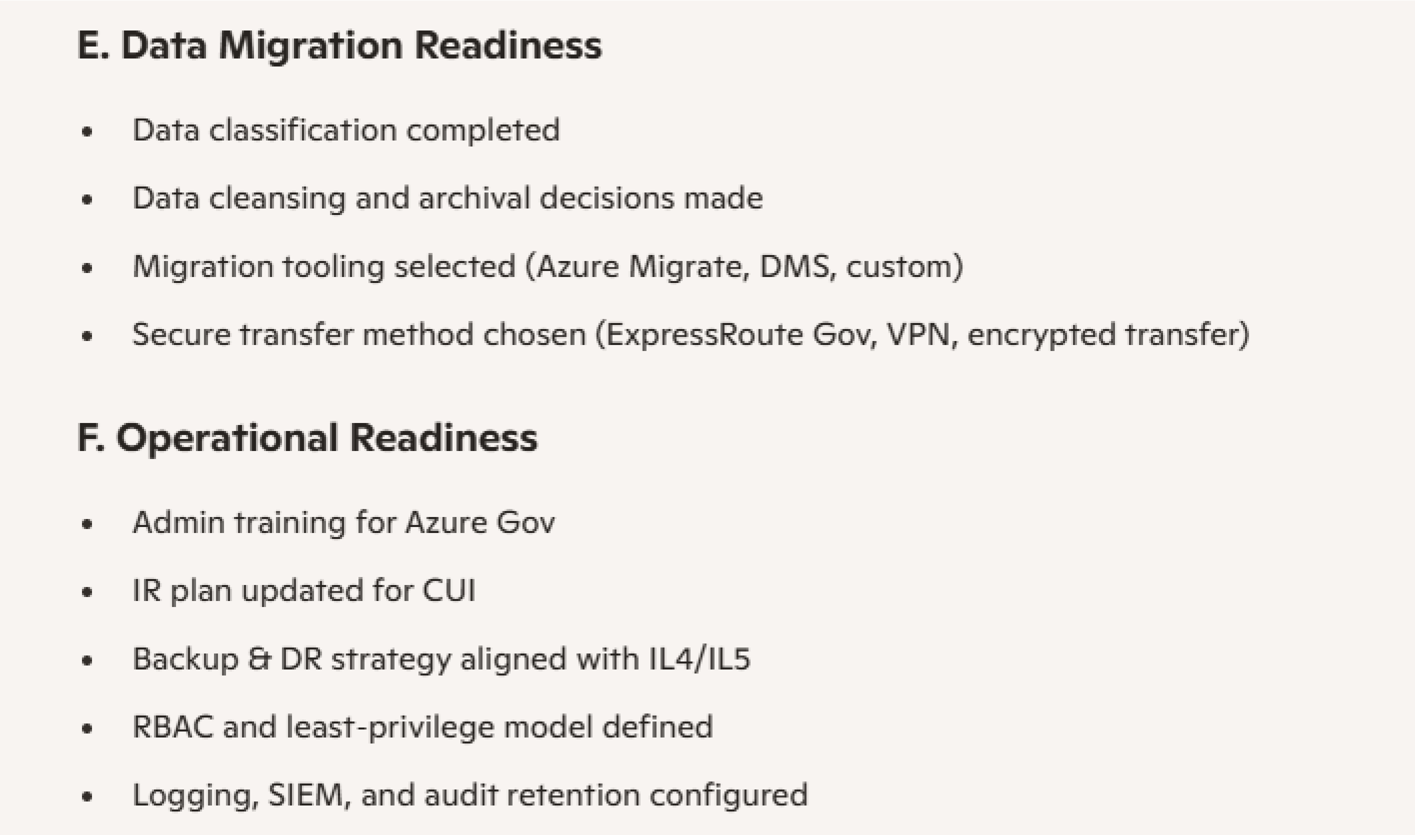


C. Security & Compliance Readiness

- SSP (System Security Plan) drafted
- POA&M created
- CMMC Level 2 control owners assigned
- Logging & monitoring requirements documented
- Data classification and retention policies defined
- Encryption requirements validated (FIPS 140-2)

D. Application & Infrastructure Readiness

- Full application inventory
- Dependency mapping (databases, file shares, integrations)
- IL4/IL5 hosting requirements identified
- Compatibility with Azure Gov services assessed
- Modernization vs lift-and-shift decision per app
- Identity integration plan (AAD, LDAP, AD DS)

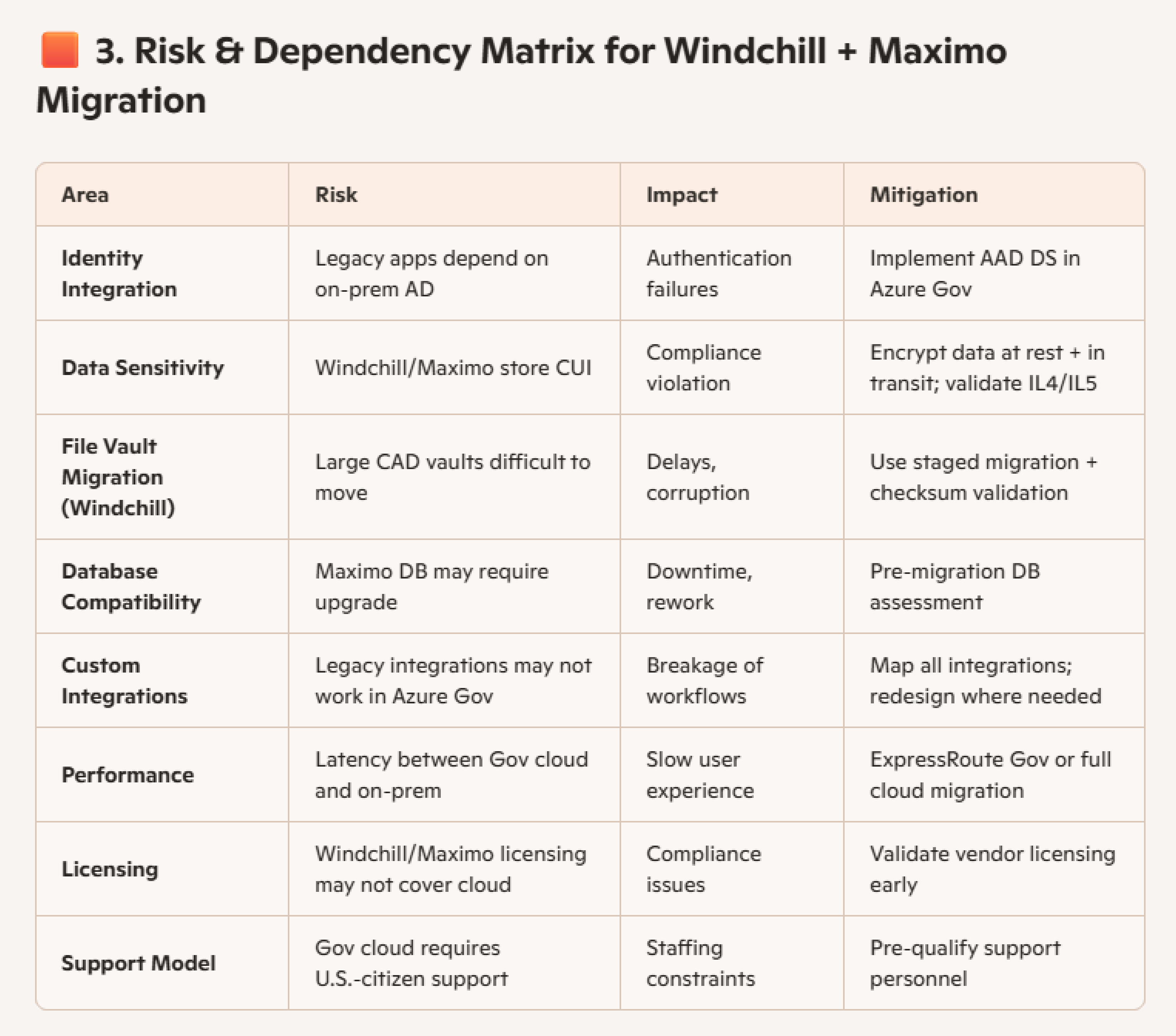


E. Data Migration Readiness

- Data classification completed
- Data cleansing and archival decisions made
- Migration tooling selected (Azure Migrate, DMS, custom)
- Secure transfer method chosen (ExpressRoute Gov, VPN, encrypted transfer)

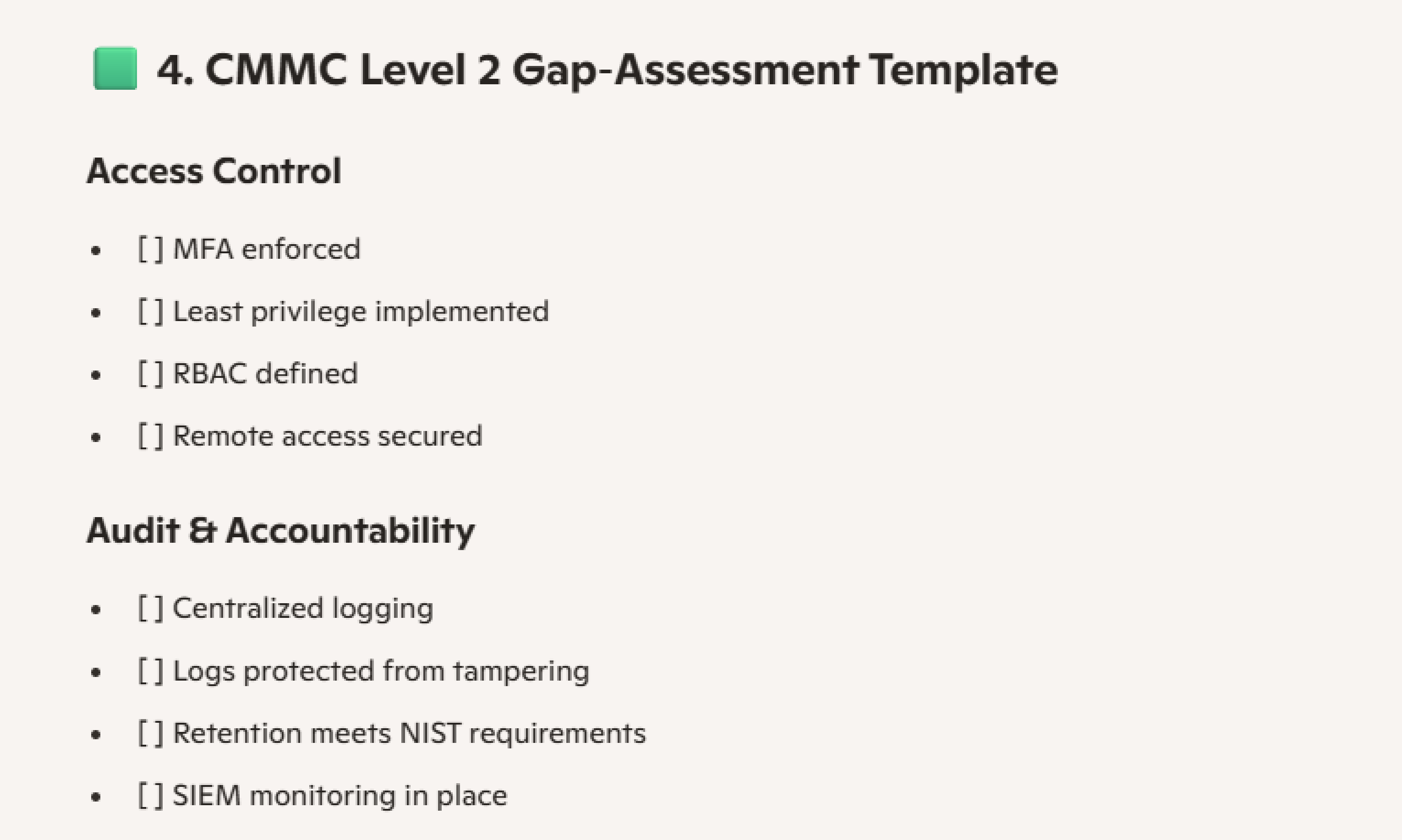
F. Operational Readiness

- Admin training for Azure Gov
- IR plan updated for CUI
- Backup & DR strategy aligned with IL4/IL5
- RBAC and least-privilege model defined
- Logging, SIEM, and audit retention configured



🟥 3. Risk & Dependency Matrix for Windchill + Maximo Migration

Area	Risk	Impact	Mitigation
Identity Integration	Legacy apps depend on on-prem AD	Authentication failures	Implement AAD DS in Azure Gov
Data Sensitivity	Windchill/Maximo store CUI	Compliance violation	Encrypt data at rest + in transit; validate IL4/IL5
File Vault Migration (Windchill)	Large CAD vaults difficult to move	Delays, corruption	Use staged migration + checksum validation
Database Compatibility	Maximo DB may require upgrade	Downtime, rework	Pre-migration DB assessment
Custom Integrations	Legacy integrations may not work in Azure Gov	Breakage of workflows	Map all integrations; redesign where needed
Performance	Latency between Gov cloud and on-prem	Slow user experience	ExpressRoute Gov or full cloud migration
Licensing	Windchill/Maximo licensing may not cover cloud	Compliance issues	Validate vendor licensing early
Support Model	Gov cloud requires U.S.-citizen support	Staffing constraints	Pre-qualify support personnel



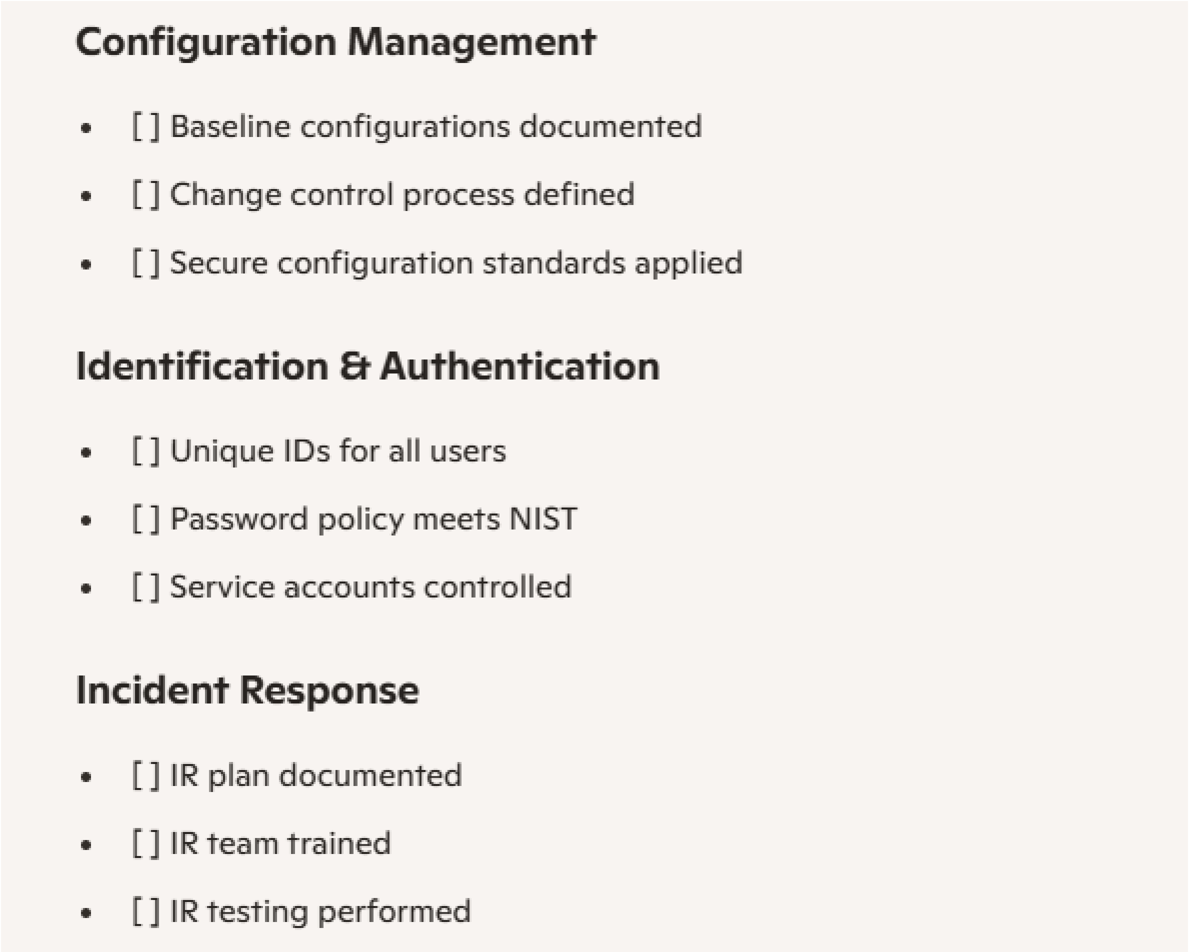
🟩 4. CMMC Level 2 Gap-Assessment Template

Access Control

- [ ] MFA enforced
- [ ] Least privilege implemented
- [ ] RBAC defined
- [ ] Remote access secured

Audit & Accountability

- [ ] Centralized logging
- [ ] Logs protected from tampering
- [ ] Retention meets NIST requirements
- [ ] SIEM monitoring in place



Configuration Management

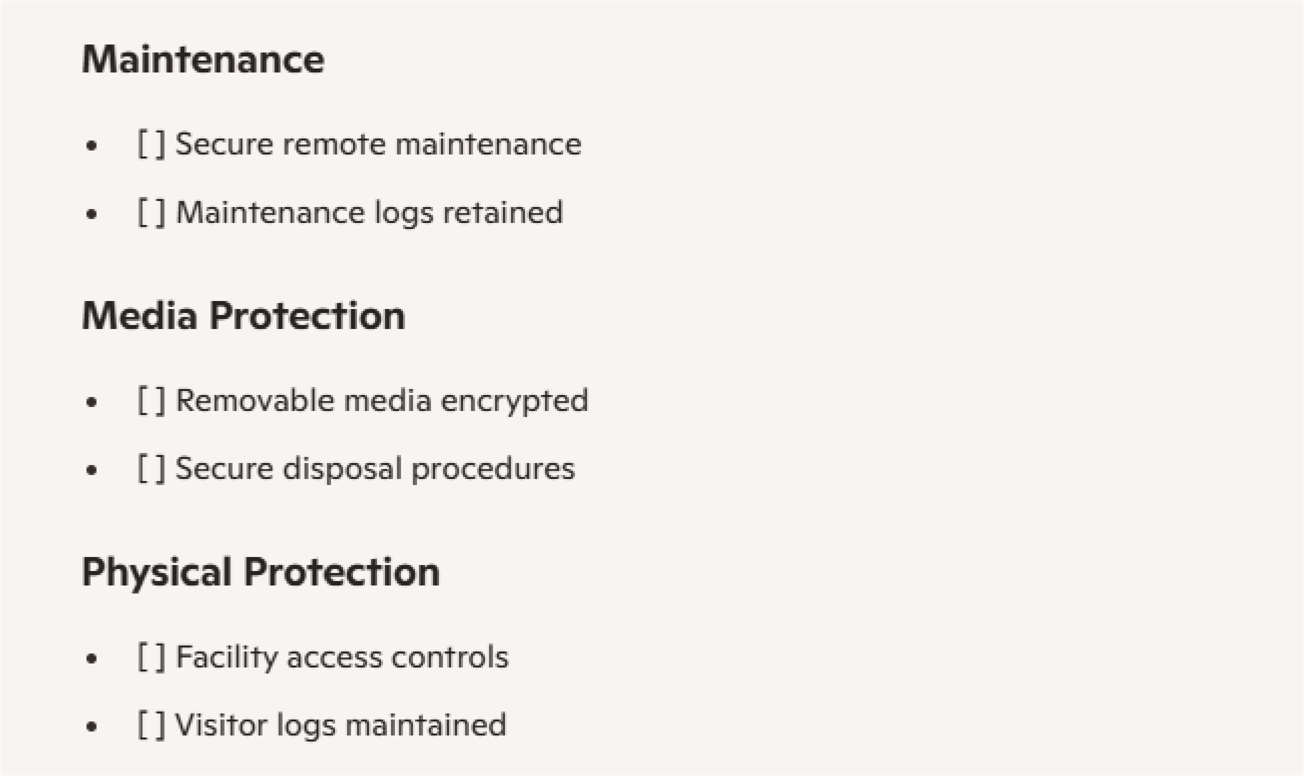
- [ ] Baseline configurations documented
- [ ] Change control process defined
- [ ] Secure configuration standards applied

Identification & Authentication

- [ ] Unique IDs for all users
- [ ] Password policy meets NIST
- [ ] Service accounts controlled

Incident Response

- [ ] IR plan documented
- [ ] IR team trained
- [ ] IR testing performed



Maintenance

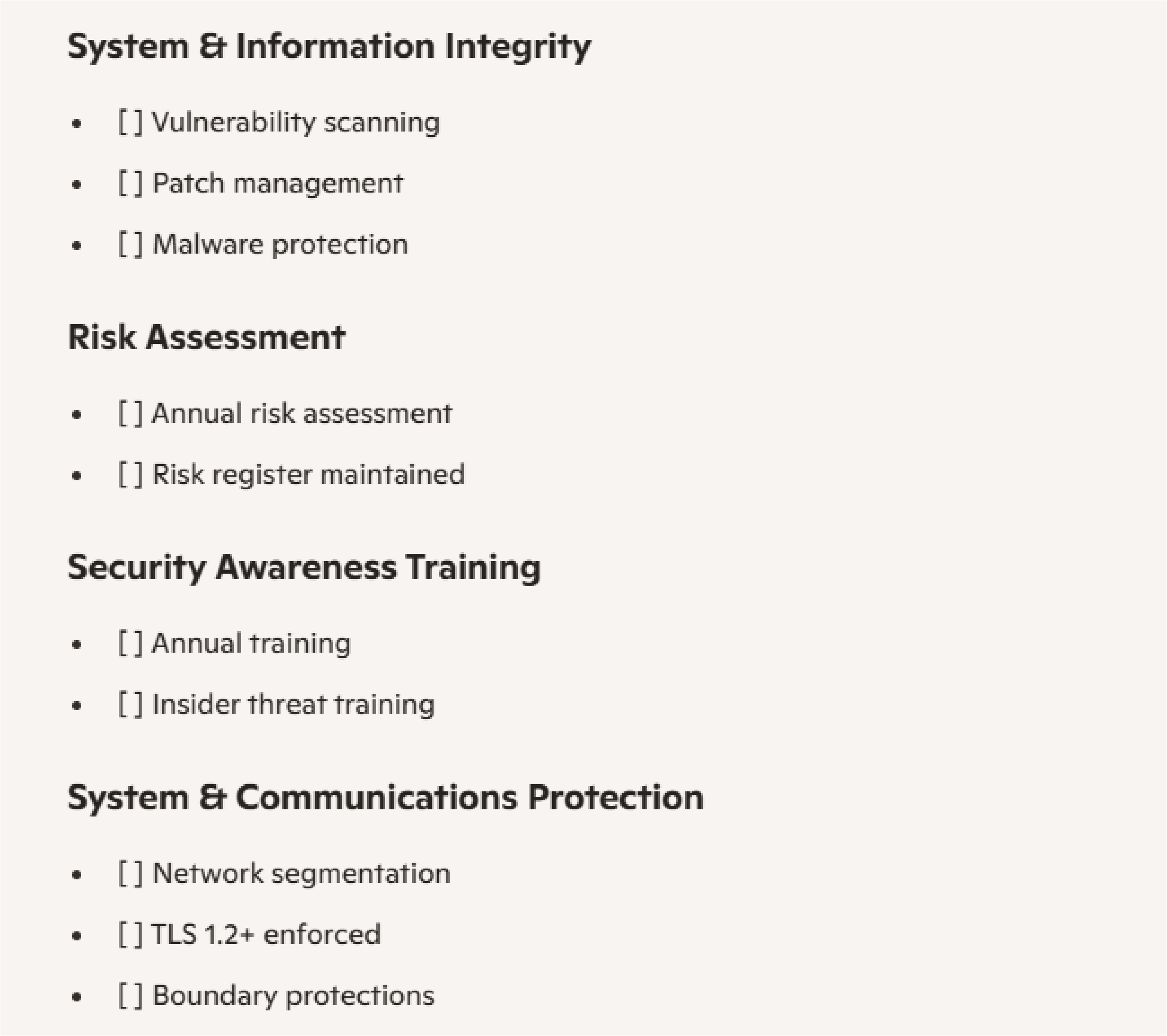
- [ ] Secure remote maintenance
- [ ] Maintenance logs retained

Media Protection

- [ ] Removable media encrypted
- [ ] Secure disposal procedures

Physical Protection

- [ ] Facility access controls
- [ ] Visitor logs maintained



System & Information Integrity

- [ ] Vulnerability scanning
- [ ] Patch management
- [ ] Malware protection

Risk Assessment

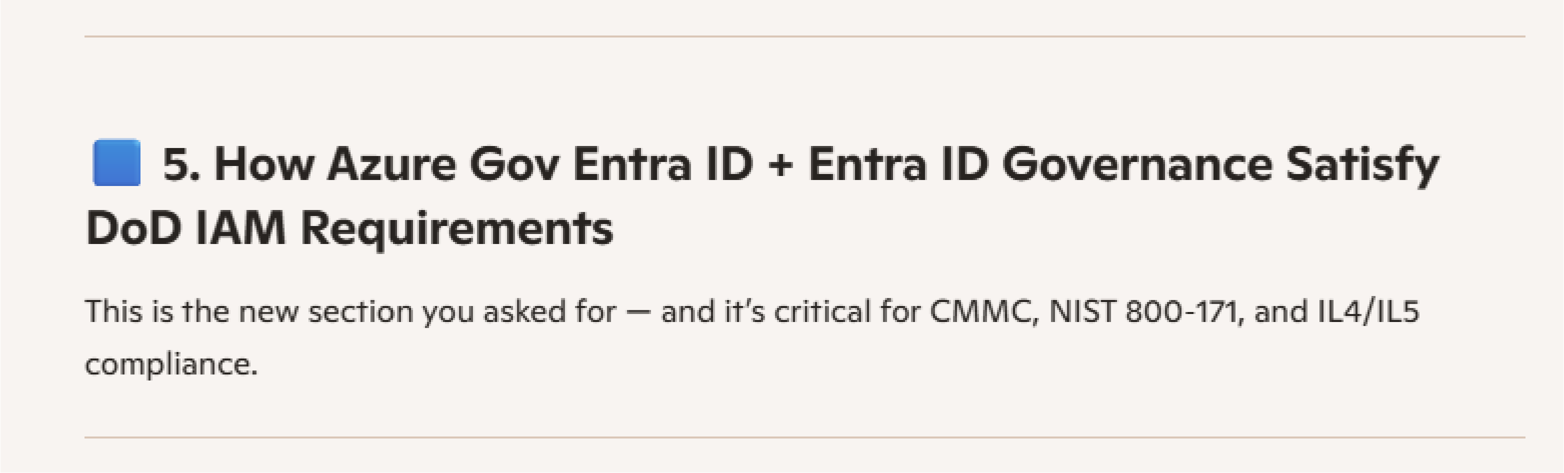
- [ ] Annual risk assessment
- [ ] Risk register maintained

Security Awareness Training

- [ ] Annual training
- [ ] Insider threat training

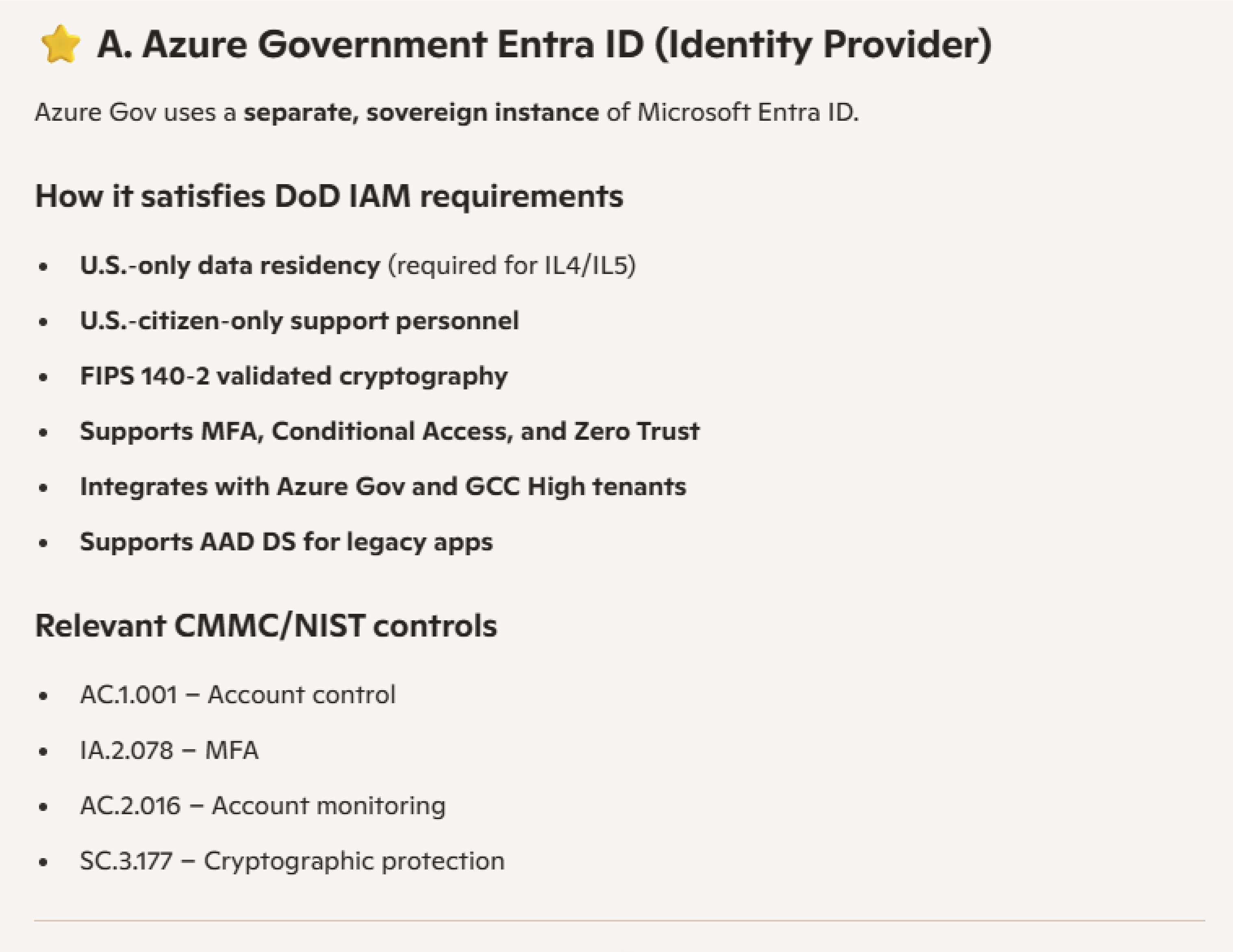
System & Communications Protection

- [ ] Network segmentation
- [ ] TLS 1.2+ enforced
- [ ] Boundary protections



🟦 5. How Azure Gov Entra ID + Entra ID Governance Satisfy DoD IAM Requirements

This is the new section you asked for — and it's critical for CMMC, NIST 800-171, and IL4/IL5 compliance.



⭐ A. Azure Government Entra ID (Identity Provider)

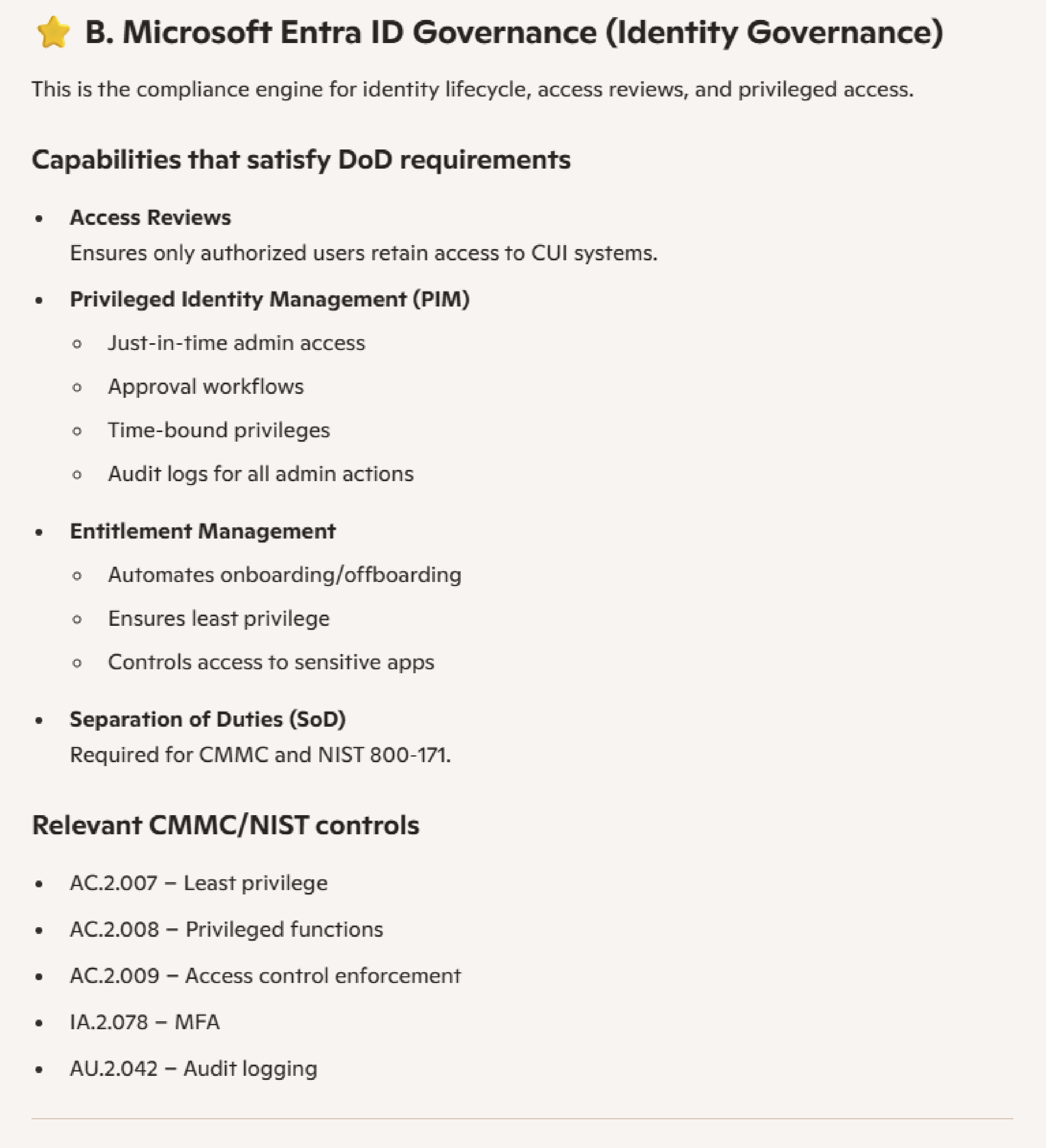
Azure Gov uses a **separate, sovereign instance** of Microsoft Entra ID.

How it satisfies DoD IAM requirements

- **U.S.-only data residency** (required for IL4/IL5)
- **U.S.-citizen-only support personnel**
- **FIPS 140-2 validated cryptography**
- **Supports MFA, Conditional Access, and Zero Trust**
- **Integrates with Azure Gov and GCC High tenants**
- **Supports AAD DS for legacy apps**

Relevant CMMC/NIST controls

- AC.1.001 – Account control
- IA.2.078 – MFA
- AC.2.016 – Account monitoring
- SC.3.177 – Cryptographic protection



⭐ B. Microsoft Entra ID Governance (Identity Governance)

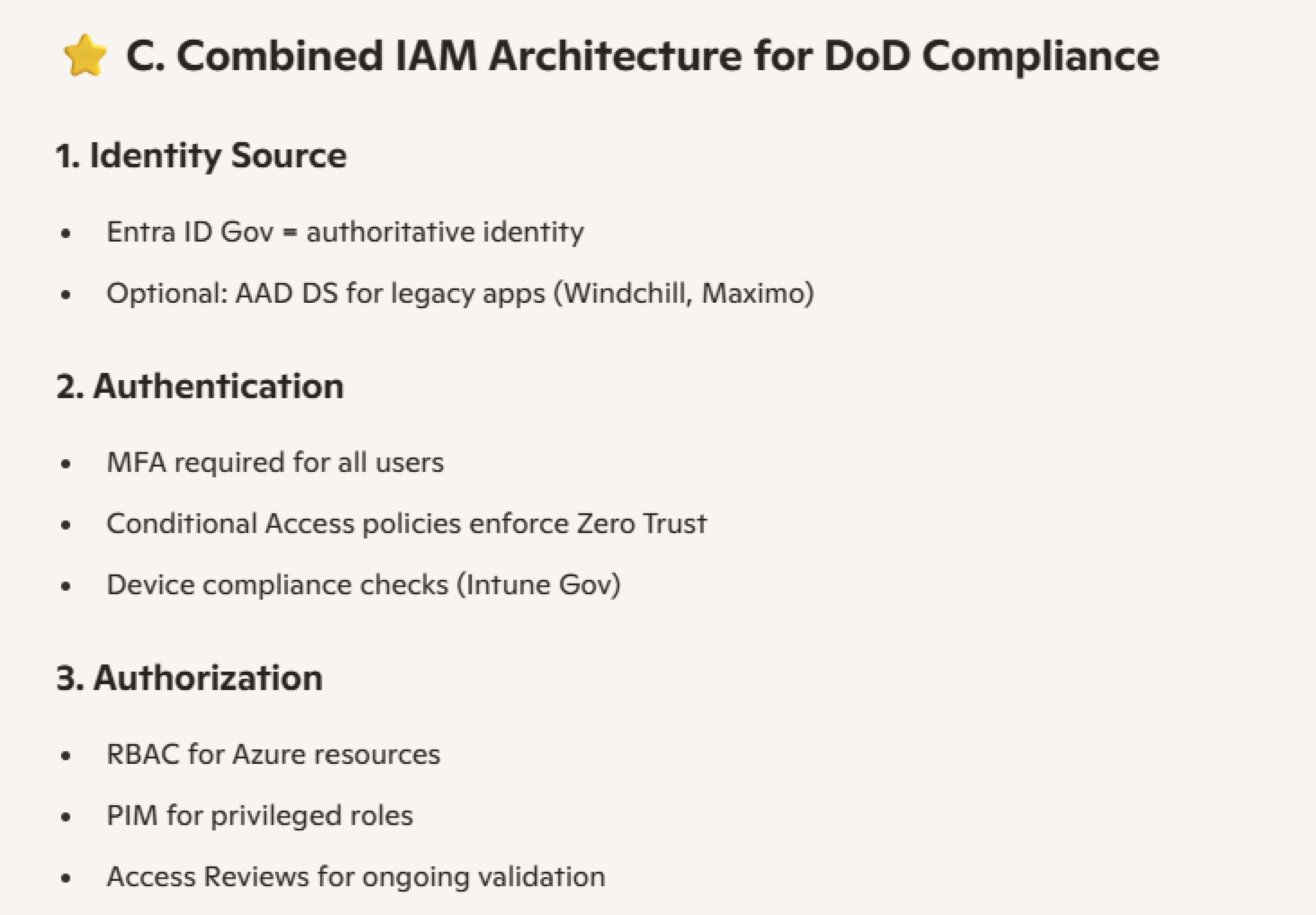
This is the compliance engine for identity lifecycle, access reviews, and privileged access.

Capabilities that satisfy DoD requirements

- **Access Reviews**
  Ensures only authorized users retain access to CUI systems.
- **Privileged Identity Management (PIM)**
  - Just-in-time admin access
  - Approval workflows
  - Time-bound privileges
  - Audit logs for all admin actions
- **Entitlement Management**
  - Automates onboarding/offboarding
  - Ensures least privilege
  - Controls access to sensitive apps
- **Separation of Duties (SoD)**
  Required for CMMC and NIST 800-171.

Relevant CMMC/NIST controls

- AC.2.007 – Least privilege
- AC.2.008 – Privileged functions
- AC.2.009 – Access control enforcement
- IA.2.078 – MFA
- AU.2.042 – Audit logging



⭐ C. Combined IAM Architecture for DoD Compliance

1. Identity Source

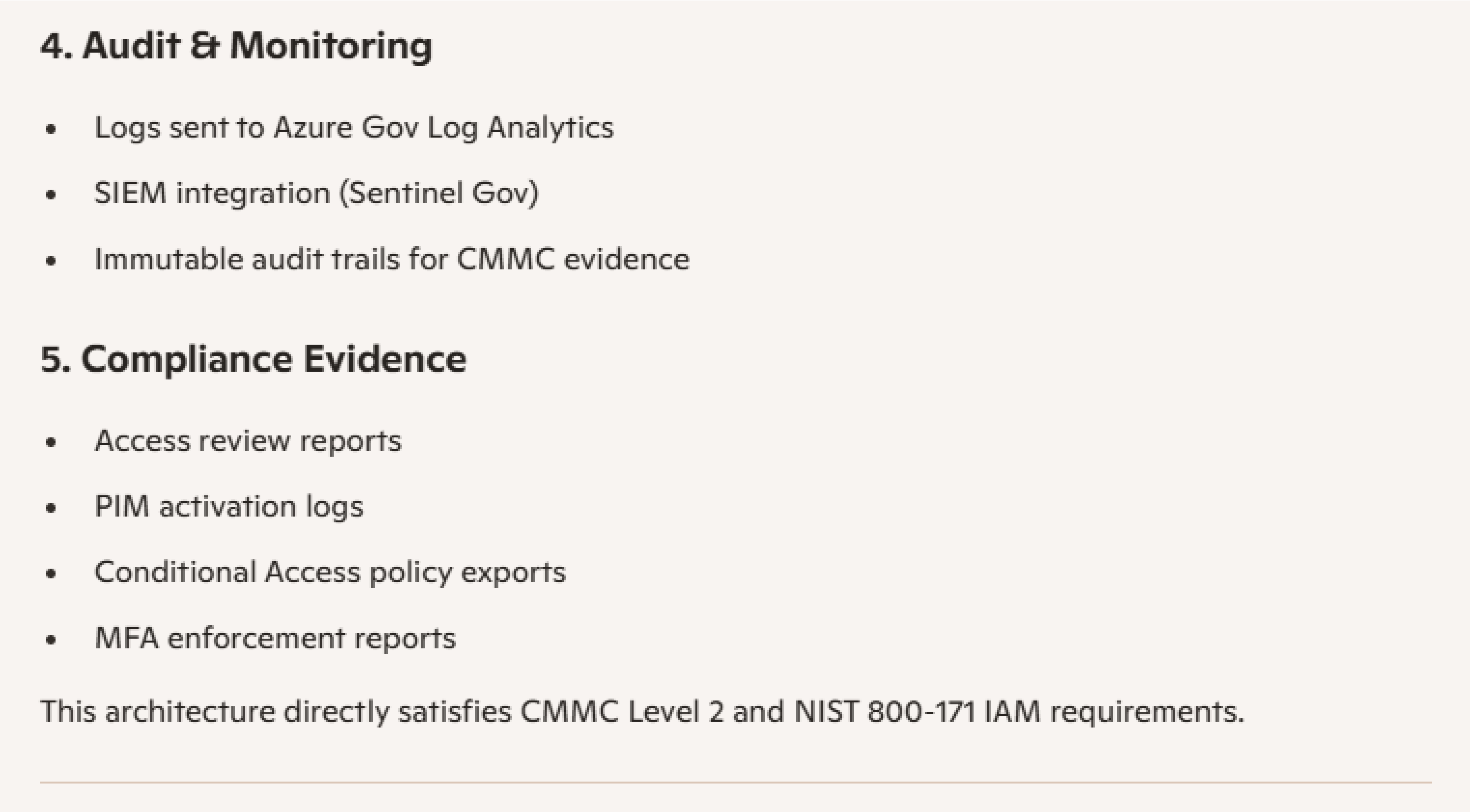
- Entra ID Gov = authoritative identity
- Optional: AAD DS for legacy apps (Windchill, Maximo)

2. Authentication

- MFA required for all users
- Conditional Access policies enforce Zero Trust
- Device compliance checks (Intune Gov)

3. Authorization

- RBAC for Azure resources
- PIM for privileged roles
- Access Reviews for ongoing validation



4. Audit & Monitoring

- Logs sent to Azure Gov Log Analytics
- SIEM integration (Sentinel Gov)
- Immutable audit trails for CMMC evidence

5. Compliance Evidence

- Access review reports
- PIM activation logs
- Conditional Access policy exports
- MFA enforcement reports

This architecture directly satisfies CMMC Level 2 and NIST 800-171 IAM requirements.

> “BUSINESS OPPORTUNITIES ARE LIKE BUSES.
> THERE'S ALWAYS ANOTHER ONE COMING.”

Richard Branson

TIMELINE

Q1 2026 Migration prep to complete

Q2 2026 Implementation phase

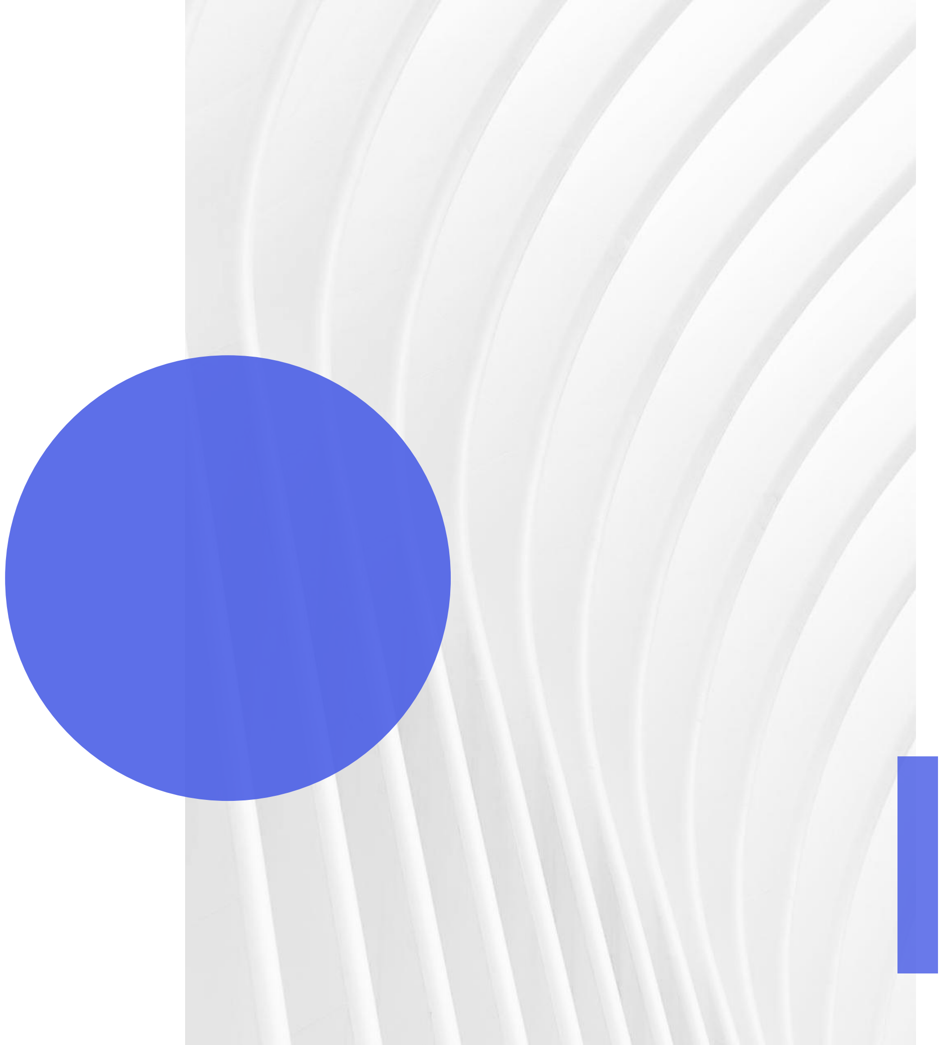
Q3 2026 Implementation phase adapting to anticipated and unanticipated changes

Q4 2026 Implementation complete

Q1 2027 Delivery and fine-tuning

SUMMARY

At Tek Systems, we don’t only meet customer’s requirements. We aim at delivering the extraordinary.



THANK YOU

Tony Shen

tshen@datacommlab.com

www.datacommlab.com