Court System Cloud Center of Excellence (CCoE) Multi-Cloud Modernization

[PLACEHOLDER: DoD Seal / Agency Logo]

Contract/Task No.: _____   Prepared For: _____   Prepared By: _____

Version: v3.0   Date: _____   Distribution: Statement D – Authorized U.S. DoD and U.S. Courts only

Document Control (Version | Date | Description | Author | Approver)

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Table of Contents

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Page 4 of 117

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Page 5 of 117

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Page 7 of 117

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Page 10 of 117

Acronyms

Acronym/Term	Definition
7R	Rehost, Replatform, Refactor, Repurchase, Retire, Retain, Relocate.
ADR	Architecture Decision Record.
Anomaly	Statistically atypical spend or usage.
ARB	Architecture Review Board.
Artifact Registry	Container/artifact storage.
ATO	Authorization to Operate.
AVM	Account Vending Machine (account factory).
Azure Policy / Initiatives	Azure governance policies/initiatives.
BOD	CISA Binding Operational Directive.
CAB/ECAB	(Emergency) Change Advisory Board.
Catalogs	Glue (AWS), Microsoft Purview (Azure), Dataplex/Data Catalog (GCP), OCI Data Catalog.
CCB	Change Control Board.
CCoE	Cloud Center of Excellence.
CDC	Change Data Capture.
CDM	Continuous Diagnostics & Mitigation (DHS).
CDRL	Contract Data Requirements List.
Chargeback/Showback	Cost allocation models.
CI	Configuration Item.
CI/CD	Continuous Integration / Continuous Delivery.
CIS	Center for Internet Security (benchmarks).
CJIS	Criminal Justice Information Services (policy domain).
Cloud Guard	OCI posture/workload protection.
Cloud Interconnect	Google Cloud dedicated connectivity.
Cloud KMS	Cloud-managed key service (generic).
CM-2/3/5/6/8	Key NIST 800-53 Configuration Management controls.
CMDB	Configuration Management Database (ITSM).
CMP	Configuration Management Plan (FedRAMP).
CNAPP	Cloud-Native Application Protection Platform.
COA	Chart of Accounts.
ConMon	Continuous Monitoring (FedRAMP).
Cosign/Sigstore	Artifact signing & provenance (Sigstore ecosystem).
CSP	Cloud Service Provider (AWS, Azure, GCP, OCI).
CSPM	Cloud Security Posture Management.
CT/CFG	AWS CloudTrail / AWS Config.
CTO	Cutover.
CUI	Controlled Unclassified Information.
CUR	Cost & Usage Report (or equivalent billing export).
CW	Court Wave (group of courts migrating together).
DC	Data Center (on-prem).
DL	Distribution List.
DLP	Data Loss Prevention.
DORA	DevOps metrics: Lead Time, Deployment Frequency, Change Failure Rate, MTTR.
DPO	Data Protection Officer / Privacy Officer.

DQ	Data Quality.
DR/BCP	Disaster Recovery / Business Continuity Plan.
DRG	Dynamic Routing Gateway (OCI).
DX	AWS Direct Connect (dedicated connectivity).
E2E	End-to-End.
EDR	Endpoint Detection & Response.
EKS/AKS/GKE/OKE	Managed Kubernetes: AWS EKS / Azure AKS / Google GKE / Oracle OKE.
Entra ID	Microsoft identity platform (formerly Azure AD).
ETL/ELT	Extract-Transform-Load / Extract-Load-Transform.
ER	Azure ExpressRoute (dedicated connectivity).
FC	Oracle FastConnect (dedicated connectivity).
FedRAMP	Federal Risk and Authorization Management Program.
FinOps	Financial Operations for cloud cost accountability.
FIPS	Federal Information Processing Standards.
FIPS 140	Cryptographic Module Security (FIPS 140-2/140-3).
FIPS 199	Security Categorization of Federal Information & Information Systems.
GitOps	Git-based ops practices/tools (e.g., Argo CD / Flux).
GPU/TPU	Accelerators; special budgeting considerations.
H2H	Host-to-Host migration.
HCD	Human-Centered Design.
IaaS	Infrastructure as a Service.
IaC	Infrastructure as Code (Terraform, Bicep, Deployment Manager).
IAM	Identity and Access Management.
IAM Policies / Dynamic Groups	Access control constructs (per cloud).
IL	(DoD) Information Impact Level.
IL5/IL6	DoD Impact Levels 5/6 — IL5 = CUI/mission-critical (unclassified), IL6 = classified up to Secret.
IL5/IL6-like	High-sensitivity handling rigor for training data & labs.
ILT/VILT	Instructor-Led Training / Virtual Instructor-Led Training.
IMS	Integrated Master Schedule.
IR	Incident Response.
ISA	Interconnection Security Agreement.
ITIL	Information Technology Infrastructure Library (v3/v4 practices).
ITOM	IT Operations Management.
ITSM	IT Service Management.
IV&V	Independent Verification & Validation.
JIT/JEA	Just-in-Time / Just Enough Access.
KEDB	Known Error Database.
Key Vault / Managed HSM	Azure key/secret services (managed HSM).
KMS/Key Vault/Cloud KMS/Vault	Key management services (per cloud).
KPI/OKR	Key Performance Indicator / Objectives & Key Results.
KSA	Knowledge, Skills, Abilities.
LMS	Learning Management System.
Log Analytics	Azure log analytics workspace / platform logging.
Logging/Monitoring (Observability)	Logs, metrics, traces & health dashboards.
LZ	Landing Zone.

Management Groups / Subscriptions	Azure hierarchy constructs.
MDM	Master Data Management.
Microsoft Defender for Cloud	Azure posture/workload protection suite.
MIM	Major Incident Management.
NACL/SG	Network ACL / Security Group.
NIST SP 800-53 Rev.5	Security & Privacy Controls for Information Systems & Organizations.
NOC	Network/Operations Center.
OIDC	OpenID Connect (workload identity for pipelines).
OPA/Rego	Policy-as-Code engine Open Policy Agent / Rego.
Org/OUs	AWS Organizations / Organizational Units.
Organization / Folders / Projects	GCP hierarchy constructs.
Organization Policy	GCP org-level governance constraints.
PaaS	Platform as a Service.
PAW/PAM	Privileged Access Workstation / Privileged Access Management.
PE/PL/PSC/SG	Private Endpoint/Private Link/Private Service Connect/Service Gateway (private PaaS access).
PII/PHI/CJIS	Sensitive data classes (personally identifiable, health, justice).
PIR	Post-Implementation Review.
PMP	Program Management Plan.
POA&M	Plan of Action & Milestones.
PoC	Proof of Concept.
PoR	Plan of Record.
PPS	Ports, Protocols & Services.
PTA/PIA	Privacy Threshold Assessment / Privacy Impact Assessment.
QASP	Quality Assurance Surveillance Plan.
RACI	Responsible, Accountable, Consulted, Informed.
RAID	Risks, Assumptions, Issues, Decisions.
RBAC/ABAC	Role-Based / Attribute-Based Access Control.
RCA/CAPA	Root Cause Analysis / Corrective & Preventive Actions.
RFC	Request for Change.
RMF	NIST Risk Management Framework (SP 800-37).
ROE	Rules of Engagement (for testing).
RTO/RPO	Recovery Time Objective / Recovery Point Objective.
SaaS	Software as a Service.
SACM	Service Asset & Configuration Management.
SAP/SAR	Security Assessment Plan / Security Assessment Report.
SARIF	Static Analysis Results Interchange Format.
SAST/SCA/DAST/IAST/RASP	Security testing approaches (Static/Composition/Dynamic/Interactive/Runtime).
SBOM	Software Bill of Materials (MLSBOM for models).
SBOM/MLSBOM	Software/Model bill of materials (supply chain).
SCA	Security Control Assessment.
SCAP	Security Content Automation Protocol.
SCIM/JIT	System for Cross-domain Identity Management / Just-in-Time provisioning.
SCORM/xAPI	E-learning content standards.
SCP	(AWS) Service Control Policy.

Security Command Center	Google Cloud posture/workload protection suite.
Security Zones	OCI security guardrail construct.
Sentinel	Microsoft Sentinel (SIEM).
SH/GD/Macie/Det/Ins	AWS Security Hub / GuardDuty / Macie / Detective / Inspector.
SIEM/SOAR	Security Information & Event Management / Security Orchestration, Automation & Response.
SIT/UAT	System Integration Testing / User Acceptance Testing.
SLA/OLA/UC	Service Level Agreement / Operational Level Agreement / Underpinning Contract.
SLI/SLO/Error Budget	Service health metrics & reliability targets.
SLSA	Supply-chain Levels for Software Artifacts (assurance framework).
SoD	Segregation of Duties.
SOP	Standard Operating Procedure.
SOW	Statement of Work.
SP	NIST Special Publication.
SP/RI/CUD/SUD	Savings Plans / Reserved Instances / Committed Use Discounts / Sustained Use Discounts.
SRE	Site Reliability Engineering.
SSDF	NIST Secure Software Development Framework (SP 800-218).
SSP/SAP/SAR/POA&M	Key RMF/FedRAMP artifacts.
STIG/CIS	DoD STIGs / CIS Benchmarks.
T3	Train-the-Trainer.
Table formats (Iceberg/Delta/Hudi)	Open table formats for data lakes.
TACoS	Total Allocated Cost of Service.
Tenancy / Compartments	OCI hierarchy constructs.
TGW	AWS Transit Gateway.
Vault	HashiCorp Vault (keys/secrets).
Virtual WAN / Hub-Spoke	Azure Virtual WAN + hub-spoke topologies.
VPC Service Controls	GCP data exfiltration protection perimeters.
WAF	Web Application Firewall.
ZT	Zero Trust (NIST SP 800-207; CISA ZTMM).
ZTA	Zero Trust Architecture.

Executive Summary

Mission

The Court Cloud Modernization Program will migrate and modernize approximately 300 independent court systems into a secure, compliant, multi-cloud ecosystem governed by a centralized Cloud Center of Excellence (CCoE).
This initiative establishes standardized governance, architecture, security, and operational guardrails across AWS, Azure, GCP, and OCI to ensure that every participating court benefits from common tooling, automated compliance, and consistent lifecycle management.

The mission aligns with DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev.5 control baselines, guaranteeing that all systems are built, monitored, and operated to the highest federal security and reliability standards.

Strategic Objectives

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

The modernization effort delivers measurable, auditable outcomes across technology, security, and operations:

Objective	Description	Measure of Success
Secure Cloud Foundations	Deploy fully compliant landing zones per cloud with shared network, security, and monitoring services.	≥98% policy compliance; conformance pack green; no critical drift >24h.
Centralized Identity & Authorization	Establish a single federated IdP with JIT/JEA, PAM, and SCIM provisioning.	100% courts federated; 0 standing privileged accounts.
Court Isolation & Data Sovereignty	Maintain dedicated account/subscription boundaries with per-court encryption keys and network segmentation.	100% Tier-1 workloads isolated; zero cross-court trust.
Data Classification & Tagging	Enforce consistent tagging (court_id, env, data_class, owner, cost_center, etc.) and lineage for Tier-1 datasets.	≥95% tag compliance; 100% Tier-1 datasets with lineage.
CI/CD & Provenance	Implement end-to-end DevSecOps pipelines with SBOM/MLSBOM and signed provenance enforcement.	100% deploys validated by provenance and attestation.
ATO-for-All Courts	Standardize RMF evidence, POA&M tracking, and continuous monitoring across all environments.	Zero overdue critical findings; assessor dry-run pass per wave.
Operational Excellence & FinOps	Integrate SRE, ITSM, and cost governance practices across environments.	MTTR <30 min; cost variance ±5%.

Scope of Work

The initiative encompasses the complete modernization lifecycle, including:

- **Landing Zones:** Standardized per-cloud architectures with SCP/Policy guardrails, centralized logging, and key management.

- **Identity & Access:** Single authoritative IdP with multi-factor authentication, privileged access workstations, and break-glass tested elevation paths.

- **Networking & Connectivity:** Dedicated circuits (DX/ER/Interconnect/FastConnect), hub-and-spoke topologies, and private access to all PaaS services.

- **Security & Compliance:** RMF/ATO alignment, FIPS 140-3 cryptography, STIG/CIS hardening, and continuous monitoring dashboards.

- **Data Platform:** Tiered Lakehouse design (Raw–Refined–Curated), DQ and lineage enforcement, data contracts, and tokenization.

- **DevSecOps:** Policy-as-Code pipelines, OIDC-based authentication, and supply-chain integrity through SBOM and SLSA compliance.

- **Operations & Resilience:** ITSM/SRE integration, DR/BCP runbooks, automated failover, and quarterly tabletop exercises.

- **Training & Change Management:** Role-based curricula, sandbox environments, and T3 enablement programs for all stakeholders.

Expected Outcomes

By program completion, all courts will operate within a **common, compliant, multi-cloud framework** that ensures:

- **Security & Compliance:** Conformance with **DoD IL4/IL5/IL6**, **FedRAMP High**, and **NIST SP 800-53 Rev.5** standards.

- **Zero-Trust Enforcement:** All administrative access via privileged workstations with continuous verification and session recording.

- **Operational Resilience:** ≥99% availability; DR tests passed quarterly; MTTR <30 minutes for P1 incidents.

- **Data Integrity & Quality:** ≥99% Data Quality (DQ) pass rate; full lineage for Tier-1 datasets.

- **Financial Accountability:** ≤±5% budget variance per phase; ≥20% optimization over baseline cost projections.

- **Governance & Transparency:** CCoE scorecards, exception tracking via ADRs, and policy compliance ≥98%.

- **Successful Migration:** 50 courts migrated by Month 12 and 300 courts operational by Month 18, with zero P1 incidents at go-live.

Program Phasing & Timeline

Phase	Duration	Key Deliverables
Phase 0 (M0–1)	CCoE Stand-up, charter approval, discovery kickoff.	CCoE charter, governance RACI, initial inventories.
Phase 1 (M1–3)	Landing Zone MVP across all clouds.	Identity federation, policy baselines, secure connectivity.
Phase 2 (M3–6)	Data Platform foundation and DevSecOps rollout.	DQ enforcement, provenance pipelines, FinOps dashboards.
Phase 3 (M6–12)	Application Platform GA; first 50 courts migrated.	Blue/green validation, ATO wave execution.
Phase 4 (M12–18)	Full 300-court migration, optimization, and DR maturity.	Continuous monitoring, cost optimization, full operational hand-off.

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Page 16 of 117

1. Objectives, Scope, and Assumptions

1.1 Objectives

The following objectives are measurable and time-bounded:

ID	Objective	Measure of Success (MoS)	Target/Date
O1	Stand up compliant landing zones in AWS/Azure/GCP/OCI	Policy compliance; conformance pack; drift-free baseline	≥98% policies green by M3 (MVP)
O2	Private access to PaaS services in all clouds	No public egress for PaaS; endpoint coverage	100% critical services via PE/PL/PSC/SG by M4
O3	Establish CCoE governance with ARB/CCB/ECAB	SOPs approved; RFC lead time; PIR completion	SOPs signed M1; RFC→PIR cycle < 14 days
O4	Data platform (lakehouse) with catalog & DQ SLAs	DQ pass rate; lineage coverage	≥99% DQ; lineage for Tier-1 datasets by M6
O5	DevSecOps pipelines with SLSA-aligned integrity	Provenance required; SBOM coverage; gate pass rate	100% deploys with provenance by M6
O6	ITSM+SRE with tested DR/BCP	DR test pass; MTTD/MTTR	Quarterly DR pass; MTTR < 30m P1
O7	Migrate courts via repeatable waves	Readiness gates; zero P1 at go-live	50 courts by M12; 300 by M18

ID	Objective	Measure of Success (MoS)	Target/Date	Owner
CC1	Multi-cloud guardrails published and enforced	≥98% policies green; no critical drifts >24h	M3	CCoE Security
CC2	Central Authorization Point live (federation, JIT/JEA, PAM)	100% courts federated; 0 standing privileged accounts	M2	CCoE Identity
CC3	Court isolation patterns in place	All tier-1 workloads isolated	M3	CCoE Platform
CC4	CI/CD with provenance & SBOM	100% deploys require provenance; SBOM 100%	M6	DevSecOps
CC5	ATO-for-All Courts program operational	0 overdue critical POA&M items	M6+	Compliance Manager
CC6	Data classification & tagging enforced	Tag compliance ≥95%; lineage for tier-1	M4/M6	Data Gov
CC7	Discovery-to-Refactor factory running	All apps categorized (7R); refactor backlog sized	M6	EA / App Leads

1.2 Scope

- Networking & connectivity (DX/ER/Interconnect/FastConnect); hub-spoke; private access; firewall policy sets.
- Observability: logging taxonomy, SIEM/SOAR, detections-as-code, dashboards, alert runbooks.

1.3 Assumptions

- Authoritative IdP (Entra ID or equivalent) federates to all clouds; M365/AAD tenant policies available.
- Court data classification policy exists; tagging scheme available for PII/PHI/CJIS/CUI.
- Connectivity (DX/ER/Interconnect/FastConnect) budgeted and orderable; interim VPN acceptable.
- Licensing for SIEM, CSPM, and pipeline scanners available or procured in Phase 1.

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

- Change freeze windows provided around court calendars; weekend cutovers allowed.
- Court SMEs available for data mapping, UAT, and sign-offs per wave calendar.
- Security team provides ROE for testing; assessor access allowed during RMF activities.

1.4 Acceptance Criteria

- Landing zones: ≥98% policy compliance; conformance pack green; drift checks scheduled.
- Identity: break-glass tested; no standing privileged accounts; quarterly access reviews complete.
- Networking: private access enforced for critical PaaS; HA failover < 60s in tests.
- Security: control narratives approved; FIPS 140-3 KMS policies; STIG/CIS scans passed.
- Observability: detections-as-code repo live; dashboards published; alert runbooks validated via game days.
- Data: DQ SLAs defined & met; lineage for Tier-1; access policies enforced via RBAC/ABAC.
- DevSecOps: provenance required to deploy; SBOM coverage 100%; gates block critical vulns.
- Operations: SOP library published; incident drills completed; DR/BCP table-tops + live tests passed.
- Migration: readiness gate checklist signed; zero P1 at go-live; reconciliation 100%.

1.5 Dependencies

- Procurement lead times for circuits (DX/ER/Interconnect/FastConnect) and HSM modules.
- Access to tenant/org root-level policy controls (SCP/Policy/Org Policy/Security Zones).
- Data source system availability for CDC; API quotas and network allowlists updated.
- Court scheduling constraints for cutovers and UAT windows.
- Availability of landing zone seed accounts/subscriptions/projects per wave.

1.6 Constraints

- Regulatory constraints: CJIS, CUI handling; region/sovereignty limits may impact placement.
- Budget ceilings per fiscal year necessitate phased commitments (SP/RI/CUD/SUD timing).
- Legacy network topologies may require interim overlay or staged migrations.

1.7 CDRLs & Key Deliverables (Section 1)

CDRL/Deliverable	Produced In	Evidence/Format
PMP/IMS	Section 1 & 17	Plan + schedule (MS Project or CSV), risks, dependencies
Scope Statement	Section 1	Signed scope doc (DOCX/PDF)
Acceptance Criteria Matrix	Section 1.4	Checklist + test results (XLSX)
KPI Registry	Section 1.10	Table (XLSX/CSV) with formulas & owners

1.8 Milestones & Exit Criteria

Milestone	Target Date	Exit Criteria
M0: Program kickoff & CCoE charter	M0+2w	Charter/RACI/SOPs approved
M1: LZ MVP (all clouds)	M1	Baseline identity/network/security deployed; policy ≥ 90%
M3: Private access to PaaS	M3	Critical services via PE/PL/PSC/SG; no public exposure

M6: Data platform foundation & DevSecOps	M6	DQ ≥99%; provenance enforced; dashboards live
M9: App platform GA	M9	EKS/AKS/GKE/OKE baseline GA; blue/green proven
M12: 50 courts migrated	M12	Zero P1 at go-live; reconciliation 100%
M18: 300 courts migrated	M18	All waves completed; optimization backlog running

1.9 RACI (Section 1 Activities)

1.10 Success Metrics / KPIs

KPI	Calculation	Target	Owner
Policy compliance	(# green policies ÷ total)	≥98%	CCoE Security
Private PaaS coverage	(# services on private ÷ critical services)	100%	Network
DQ pass rate	(# checks passed ÷ checks run)	≥99%	Data
Provenance coverage	(# releases with attestations ÷ total releases)	100%	DevSecOps
SLO attainment	(% of periods within SLO)	≥99%	SRE
Cost variance	((Actual-Budget) ÷ Budget)	±5%	FinOps
Wave on-time	(# waves on schedule ÷ total)	≥90%	PMO

2. Governance: CCoE, RACI, Controls CCoE Charter

- Mandate: policy, patterns, guardrails; own ARB/CCB/ECAB; steward FinOps & training.
- Composition: Enterprise Arch, Security, Network, Data, Platform, FinOps, Operations, PMO.

2.1 RACI (Excerpt)

Activity	R	A	C	I
Define guardrails (SCP/Policy/Org Policy/SecZones)	CCoE Security	CISO	Cloud Platform	Court IT
Approve landing zone patterns	Enterprise Architect	CTO	Security, Network	PMO
Budget & optimization governance	FinOps Lead	CFO	CCoE, Platform	Court Leads

2.2 Governance Processes

- ARB/CCB/ECAB cadence and quorum; RFC intake, evaluation, approval, and PIR closure.
- Change windows aligned to court calendars; emergency change pathways documented.

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

2.3 Control Framework

2.4 Central Authorization Point (IdP/SSO + Court Isolation)

Establish a single authoritative IdP with federation to AWS/Azure/GCP/OCI. Enforce MFA for admins, JIT/JEA for elevation, SCIM/JIT for provisioning, and PAM with approvals + session recording. All court access flows through this point; no direct local admins.

Checklist Item   Status (☐/☑)   Evidence / Link Owner   Notes

Checklist Item	Status	Owner
IdP trusts in all clouds; MFA enforced for privileged roles	☐	Identity Lead
SCIM/JIT enabled; quarterly access review cadence	☐	Identity Lead
PAM integration with approvals + session recording	☐	Security
Per-court isolation mapping (accounts/subscriptions/projects/compartments)	☐	Platform
Break-glass tested; audit immutability verified	☐	Security

- Map NIST SP 800-53 Rev.5 to cloud services & IaC policies; maintain control narrative.
- Policy-as-Code enforcing least privilege and drift detection across all clouds.
- ARB/CCB/ECAB integrated with RFC/PIR; KEDB for problem management.

2.4 Deliverables

- CCoE Charter; RACI; Policy Catalog; ARB/CCB/ECAB SOPs; RFC/PIR templates; Governance Comms Plan.

3. Multi-Cloud Architecture Strategy & Decisions

3.1 Workload Placement Matrix (Excerpt)

Driver	AWS	Azure	GCP	OCI
Existing contracts/tools	★★★	★★★	★★	★★
Data sovereignty / VPC-SC needs	★★	★★	★★★	★★
Oracle workloads	★	★	★	★★★
Microsoft integration (Entra/Defender)	★★	★★★	★★	★
Analytics/BigQuery pattern	★	★	★★★	★
Cost/commit discounts	★★★	★★★	★★★	★★★

3.2 Environment Discovery (Hardware/Software) & Refactor Tracks

Perform discovery of hardware, software, and integrations. Produce per-court inventories, risk registers, and 7R decisions; create refactor tracks where modernization is required.

Discovery Area Tooling/Inputs   Output Owner

Discovery Area	Discovery Area	Discovery Area	Discovery Area

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Compute / VMware	RVTools, vROps, PowerCLI, CMDB	VM inventory; OS & patch levels; HA / DRS / vSAN status	Infrastructure
Network	Firewalls, routers, IPAM, NetFlow	VLAN and CIDR plans; ACL, NAT, DMZ; egress / ingress maps	Network
Security	EDR, SIEM, vulnerability scans	Control gaps; findings and exceptions	Security
Applications	Interviews, APM, dependency maps	Service maps; SLAs; data sensitivity; 7R candidacy	EA / Applications
Storage / Backup	Backup systems, RPO / RTO configs	Restore viability reports; cloud archive plans	Storage

Acceptance: readiness report per court including inventories, risk/gaps, 7R decision, and refactor backlog with estimates.

3.2 Service Model Selection
- IaaS for bespoke stacks
- PaaS for managed DB/analytics/integration
- SaaS where feasible to reduce TCO

3.3 Golden Patterns
- Private access: PE/PL/PSC/Service Gateway
- KMS/Key Vault/Cloud KMS/Vault with BYOK/HYOK
- CSPM/CWPP + SIEM/SOAR integration

3.4 Decision Trees & Exceptions
- If sovereignty/egress constraints → prefer GCP with VPC-SC perimeters for analytics.
- If Oracle core workloads → prefer OCI while keeping cross-cloud logging and identity parity.
- Escalate exceptions via ARB; record ADR with rationale and sunset date.

4. Landing Zones (Per Cloud)

Expanded Details

Purpose
- Define regulator-ready landing zones across AWS, Azure, GCP, and OCI to onboard 300 courts with strict tenancy isolation and centralized CCoE governance.

Scope & Assumptions
- Per-court isolation (one account/subscription/project/compartment) with separate shared services estates.
- Provisioning through IaC and policy-as-code; no public ingress by default; private access patterns enforced.

Architecture
- AWS: Organizations/OUs with SCPs; Control Tower/AVM; hub-spoke VPCs via TGW; PrivateLink; DX; centralized KMS/CloudHSM; immutable logging.
- Azure: Management Groups; Policy/Initiatives; ALZ patterns in Bicep; Virtual WAN/hub-spoke; Private Link; ExpressRoute; Key Vault/HSM.

- GCP: Org/Folders/Projects; Org Policy; Project Factory; Shared VPC; Dedicated Interconnect; Private Service Connect; VPC-SC perimeters.
- OCI: Tenancy/Compartments; Security Zones; DRG; FastConnect; Service Gateway; Vault (KMS/HSM).

Deliverables

- Terraform/Bicep modules (OU/SCP/VPC/TGW; MG/Policy; Org Policy; Compartments); vending SOP; conformance tests; golden patterns.

Acceptance

- Conformance packs green; policy compliance ≥ 98%; drift-free baselines; break-glass procedure tested; private-only data planes.

AWS

- Org/OUs, SCP, AVM; logging/monitoring accounts; centralized KMS/HSM.
- Networking: TGW; hub-spoke VPCs; PrivateLink; DX; egress control.
- Security: CT/CFG, Security Hub/GuardDuty/Macie/Detective/Inspector; WAF; key rotation.
- Deliverables: IaC modules (OU/SCP/VPC/TGW), runbooks, account vending SOP.
- Acceptance: conformance pack pass, drift-free baseline, break-glass tested.

Azure

- Management Groups/Subscriptions; Policy/Initiatives; Blueprints.
- Networking: Virtual WAN/Hub-Spoke; Private Link; ExpressRoute.
- Security: Defender for Cloud; Sentinel; Key Vault/HSM; WAF; Log Analytics.
- Deliverables: Bicep/Terraform modules; MG hierarchy; policy assignments.
- Acceptance: Policy compliance ≥ 98%, secure score targets met.

GCP

- Org/Folders/Projects; Org Policy; Project Factory.
- Networking: Shared VPC; Dedicated Interconnect; Private Service Connect.
- Security: VPC Service Controls; Security Command Center; Cloud KMS.
- Deliverables: Terraform modules; perimeter definitions; service directory.
- Acceptance: VPC-SC enforced on sensitive projects; org policy tests green.

OCI

- Tenancy/Compartments; Security Zones; Compartment factory.
- Networking: DRG; FastConnect; Service Gateway; NSGs.
- Security: Vault (KMS/HSM); Cloud Guard; Events/Alarms.
- Deliverables: Terraform modules; compartment model; policy sets.
- Acceptance: Security Zones clean; key management validated.

Operational Access	PAW; JIT elevation with approvals	PAM logs
Data Boundaries	Per-court KMS keys; separate buckets; VPC-SC/Security Zones	Key/storage policies

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Page 22 of 117

Network Segmentation   Hub-spoke + firewalls + RPZ; egress controls   Firewall configs, RPZ exports

Identity Isolation Per-court groups and role bindings; no cross-court standing access   Role/Group exports

Control Implementation Evidence

Implement strict isolation per court via separate accounts/subscriptions/projects/compartments, segmented networks, dedicated keys/log buckets, and RBAC/ABAC-only access. Deny transitive trust by default; all PaaS access is private (PE/PL/PSC/Service Gateway).

4.5 Court Isolation Policy & Controls

4.5 Court Isolation Policy & Controls

Purpose. Enforce strict **per-court isolation** across identity, network, data, and operations so no court can impact another. Every court operates within its **own cloud boundary** (accounts/subscriptions/projects/compartments) with private service access, dedicated keys, and zero transitive trust.

4.5.1 Objectives

- **Hard boundaries:** One boundary per court (no shared prod tenants).
- **Zero transitive trust:** No cross-court access paths by default.
- **Private PaaS only:** All service access via PE/PL/PSC/Service Gateway.
- **Dedicated crypto & logs:** Per-court KMS keys and log buckets.
- **Auditable operations:** JIT/JEA elevation; PAW for admins; immutable logs.

4.5.2 Architecture & Boundaries

Layer	Isolation Standard	Notes
Identity	Per-court groups/roles; no cross-court standing access	All admin paths via PAW and JIT/JEA.
Accounts/Tenancy	One AWS Account / Azure Subscription / GCP Project / OCI Compartment per court	Seeded by AVM/Factory; tagged court_id.
Network	Hub-spoke; per-court spokes; L3/L7 firewalls; RPZ; egress control	No peering between courts. Shared hub provides egress inspection only.
Data	Per-court encryption keys, buckets, databases	Separate KMS/Key Vault/Cloud KMS/Vault keys.
Observability	Per-court log buckets + central SIEM	Write-once/immutable store; tenant-scoped readers.
PaaS Access	Private endpoints only (PE/PL/PSC/SG)	No public endpoints exposed.

4.5.3 Controls Matrix (What & How)

Control Domain	Implementation	Evidence
Identity Isolation	Court-scoped groups, roles, dynamic groups; deny cross-court role grants	Role/Group exports; access reviews; IdP policy
Network Segmentation	Per-court spokes, dedicated subnets; NGFW; RPZ; egress allow-listing	Firewall configs; RPZ exports; NAT/ACL rules

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Data Boundaries	Per-court keys; separate storage; service perimeters (where supported)	Key policies; bucket policies; perimeter defs
Operational Access	PAW; JIT/JEA via PAM approvals and session recording	PAM logs; approval records; session playback
Private PaaS	PE/PL/PSC/SG to all critical services	Endpoint inventories; deny public checks
Observability	Court logs to WORM/immutable storage; central SIEM views	Retention/Lifecycle configs; SIEM dashboards

4.5.4 Enforcement (Policy-as-Code)

- **Tagging required** on **all** resources: court_id, env, owner, data_class, cost_center.
- **Create/Update Deny** if required tags missing or **if public endpoints** are enabled on managed services.
- **Key usage policies** restrict decryption to resources with matching court_id.
- **Pipeline gates** block deployments that target a court boundary without provenance/SBOM.

4.5.5 Operational Procedures

1. **Provision** court boundary via account/subscription/project/compartment factory (AVM/Project Factory/Compartment Factory).
2. **Bind identity**: create court roles/groups; assign least-privilege; register in IdP (SCIM/JIT).
3. **Lay down network**: create spokes, attach to hub; program firewalls and RPZ; configure private PaaS endpoints.
4. **Enable keys & logs**: create per-court keys; set storage/logging with WORM; connect SIEM.
5. **Activate controls**: attach policy packs; enable drift/conformance checks; onboard to PAM/PAW.
6. **Validate** with isolation tests (see 4.5.6) before any workload cutover.

4.5.6 Testing & Validation

Test	Method	Pass Criteria
Cross-Court Access	Attempt role assume / API from Court A → Court B	Access denied; audit log captured
Public Exposure	Scan for public endpoints / storage	0 public endpoints; exceptions approved
Private PaaS	Service access test without public internet	Success via PE/PL/PSC/SG only
Key Isolation	Try decrypt with mismatched court_id	Denied; event logged
Egress Control	Egress to non-approved destinations	Blocked; alert in SIEM
Break-Glass	Simulate break-glass elevation	Works with approval; full session recorded

4.5.7 Acceptance Criteria (Section 4.5)

- 100% **court boundaries** deployed with required tags and policy packs.
- **0** cross-court access paths detected.
- **0** public endpoints on critical services.
- All PaaS traffic over private endpoints.
- Break-glass elevation **tested**; PAW enforced for admins.
- Evidence artifacts present (see 4.5.8).

4.5.8 Evidence Artifacts (Per Court)

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

- Role/Group export (CSV/JSON); quarterly access review report.
- Firewall/RPZ configs; NAT/ACL exports.
- Key policies; storage/bucket policies; perimeter definitions.
- PAM session logs; approvals; PAW attestation.
- Endpoint inventories (PE/PL/PSC/SG); public-exposure scans.
- SIEM dashboards & alert history; drift/conformance pack reports.

4.5.9 RACI (Excerpt)

Activity	R	A	C	I
Provision court boundary	Platform	CTO	Security, Network	Court IT
Identity & role setup	Identity	CISO	Platform	Court IT
Network segmentation & RPZ	Network	CISO	Security	Platform
Private PaaS enablement	Platform	CTO	Network	App Teams
Keys & logging setup	Security	CISO	Data, Platform	Court IT
Isolation testing	Security	CISO	Platform, Network	PMO

4.5.10 Exceptions & Waivers

- Exceptions require **ARB/CCB approval**, a **time-boxed waiver**, and **compensating controls**.
- All exceptions tracked via **ADR** with sunset date; reported on the **CCoE scorecard**.

4.5.11 Per-Cloud Mapping (Quick Reference)

Cloud	Boundary Construct	Private PaaS	Perimeter / Guardrail
AWS	Account, OU/SCP	PrivateLink	SCP + AWS Config + Security Hub
Azure	Subscription, Mgmt Groups	Private Link	Azure Policy / Initiatives
GCP	Project, Folder	Private Service Connect	Org Policy + VPC Service Controls
OCI	Compartment, Tenancy	Service Gateway	Security Zones + Cloud Guard

4.5.12 Court Isolation Checklist (Wave Sign-off)

- ☐ Court boundary created; tags present (court_id, env, …)
- ☐ Roles/groups applied; quarterly access review scheduled
- ☐ Spoke VNET/VPC/VPC-Network built; hub connectivity and firewalls configured
- ☐ Private endpoints to all critical PaaS established
- ☐ Keys/logging configured (WORM/immutable)
- ☐ Public exposure scan = clean
- ☐ Isolation test pack executed; results attached
- ☐ Break-glass drill completed; session logs archived

5. Identity and Access

- Centralize identity and enforce least-privilege with JIT/JEA, PAW, and PAM; eliminate long-lived credentials.
- Single authoritative IdP (e.g., Entra ID) federating to all clouds; SCIM/JIT for provisioning; OIDC for workloads.
- Role catalog per court and CCoE; scoped roles by tenant unit; privileged elevation via PAM with session recording; immutable audit logs.
- IdP trusts; SSO runbooks; SCIM mappings; role catalogs; break-glass SOP; quarterly access review cadence.
- No standing privileged accounts; access certifications complete; audit logs immutable and centrally retained.
- Federation via Entra ID/IdP; OIDC for workloads; SCIM/JIT for provisioning.
- Role catalog & least-privilege baselines; JIT/JEA; PAW for admins; PAM with approvals.
- Deliverables: IdP trusts, SSO runbooks, role catalogs, break-glass process, quarterly access review cadence.
- Acceptance: no standing privileged accounts; access certifications completed; audit logs immutable.

Acceptance: current packets for all courts; zero overdue critical POA&M; assessor dry-run pass for first 5 courts per wave.

Packet Component	Packet Component	Packet Component	Packet Component
SP	System Security Plan with court boundary and controls	DOCX / XML	Annual + Change
SCTM	Security Control Traceability Matrix	XLSX	Quarterly
PPSM	Ports / Protocols with approvals	XLSX	Quarterly
STIG / CIS	Baseline hardening evidence	CKL / PDF	Quarterly
Vulnerability Scans	Recent scans and remediation	PDF	Monthly
POA&M	Open findings with mitigations and target dates	XLSX	Monthly
ConMon	Continuous Monitoring dashboards	DOCX	Monthly
IR / DR	Incident & DR test evidence	DOCX / PDF	Quarterly

Standardize RMF/ATO with reusable narratives and evidence; maintain per-court boundary packets and continuous monitoring.

5A. ATO-for-All Courts (Program Plan)

Standardize RMF/ATO across all courts using reusable narratives, shared evidence, and continuous monitoring. Each court maintains a boundary packet; the CCoE governs process, cadence, and quality, ensuring assessor-ready artifacts at all times.

5A.1 Objectives

- **Consistency:** One RMF/ATO playbook, reusable narratives, and common controls mapping.
- **Speed:** Pre-approved patterns and evidence reduce per-court prep time.
- **Assurance:** Continuous Monitoring (ConMon) with monthly evidence refresh; zero overdue critical POA&M items.

5A.2 RMF/ATO Packet (Per Court)

Packet Component	Description	Template / Format	Cadence
SSP	System Security Plan with court boundary, system description, and implemented controls	DOCX / XML	Annual + Change
SCTM	Security Control Traceability Matrix (control → evidence → status)	XLSX	Quarterly
PPSM	Ports/Protocols/Services with approvals and justifications	XLSX	Quarterly
STIG / CIS	Baseline hardening evidence and scan outputs	CKL / PDF	Quarterly
Vulnerability Scans	Current authenticated scans and remediation status	PDF	Monthly
POA&M	Findings, mitigations, due dates, ownership	XLSX	Monthly
ConMon	Continuous monitoring dashboards + data feeds	DOCX (dashboard snap)	Monthly
IR / DR	Incident records, DR tests, lessons learned	DOCX / PDF	Quarterly

Acceptance: Current packet for every court; **zero overdue critical POA&M**; assessor **dry-run pass** for first five courts in each wave.

5A.3 Roles & RACI (Excerpt)

Activity	R	A	C	I
Maintain ATO playbook/templates	CCoE Compliance	CISO	Security, Platform	Courts
Produce per-court SSP & SCTM	Court ISSO	Court CIO	CCoE Compliance	Assessor
ConMon dashboards + data feeds	Security Ops	CISO	SRE, Platform	Courts
POA&M triage & tracking	Court ISSO	Court CIO	CCoE Compliance	Assessor
Assessor dry-run (per wave)	CCoE Compliance	CISO	Court ISSO, Platform	PMO

5A.4 Process & Cadence

1. **Initialize** (M0–M1): Issue templates; align control inheritance (CSP vs. customer).
2. **Baseline** (M1–M3): Create SSP/SCTM; import STIG/CIS; run initial vuln scans; stand up ConMon feeds.
3. **Operate** (Monthly/Quarterly): Refresh scans; update POA&M; publish ConMon snapshots; perform IR/DR evidence updates.
4. **Assess** (Per Wave): Dry-run with assessor; remediate; collect sign-offs; proceed to formal authorization as required.

5A.5 Evidence Repository (Per Court)

/evidence/<court_id>/
 SSP/
 SCTM/

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

STIG_CIS/
Vuln_Scans/
POAM/
ConMon/
IR_DR/
Attachments/ (ISA, ISAAs, MoUs, waivers)

- **Retention:** 1 year minimum for scan reports, POA&M history, and ConMon snapshots.
- **Integrity:** Evidence stores are versioned and access-controlled (RBAC/ABAC) with audit logging.

5A.6 KPIs

- **POA&M Timeliness:** 100% of critical items within due date.
- **Evidence Freshness:** ≥ 95% artifacts within cadence window.
- **Assessor Dry-Run:** ≥ 90% findings informational/minor; no critical blockers.
- **ConMon Coverage:** 100% Tier-1 systems reporting.

6. Networking and Connectivity
- Provide secure, performant connectivity with private access to PaaS and validated HA failovers.
- Non-overlapping IPAM per court; DNS strategy with RPZ; dual-carrier circuits where required; encrypted overlays allowed.
- Hub-and-spoke with central inspection; regional hubs per cloud; registry access via private endpoints; QoS/bandwidth mgmt; automated failover testing.
- L3/L7 policy sets; routing designs; firewall rulebooks; runbooks for cutover/failback; packet capture SOP.
- Packet loss < 0.1%; failover < 60s; no public ingress paths; DNS resolution integrity verified.
- IPAM & address plans per court; DNS/RPZ strategy; egress controls and NAT.
- DX/ER/Interconnect/FastConnect designs; HA testing; QoS and bandwidth mgmt.
- Private access to PaaS (PE/PL/PSC/Service Gateway); registry access via private endpoints.
- Deliverables: L3/L7 policy sets, routing design, firewall rulesets, runbooks.
- Acceptance: packet loss < 0.1% in tests; failover switchover < 60s.

7. Security, Compliance, RMF/ATO
- Achieve ATO with inheritable controls and continuous monitoring.
- RMF lifecycle with evidence automation; control inheritance catalog (CSP vs customer).
- FIPS 140-3 crypto; STIG/CIS baselines; CJIS/CUI handling; ConMon dashboards and evidence pipelines.
- SSP/SAP/SAR/POA&M; ISA; PPS; PTA/PIA; control narratives; assessor dry-run kit.
- Assessor dry-run passed; POA&M triaged; ConMon dashboards live with thresholds.
- RMF stages with evidence capture; control matrix; inherited vs customer controls.
- FIPS 140-3 crypto; STIG/CIS baselines; CJIS/CUI handling; ConMon plan.
- Deliverables: SSP/SAP/SAR/POA&M; ISA; PPS; PTA/PIA; control narratives.
- Acceptance: assessor dry-run passed; POA&M findings triaged; ConMon dashboards live.

8. Logging, Monitoring, and Observability

- Unified observability with SLOs, detections-as-code, and SOC integration.
- Centralized storage per cloud with immutability; cross-region replication; alert policy standards.
- Detections-as-code repo; synthetic probes; dashboards per domain; noise reduction backlog; PIR template.
- Detections library; dashboards; alert runbooks; PIR template.
- Mean alert ACK < 5m; top 20 detections validated; PIRs closed with CAPA.
- Logging taxonomy & retention matrix; centralized storage + SIEM; detections library.
- SLOs, SLIs, error budgets; alert severity & on-call rotations; synthetic probes.
- Deliverables: detection-as-code repo; dashboards; alert runbooks; PIR template.
- Acceptance: mean alert acknowledgment < 5m; top 20 detections validated.

9. Data Platform (Lakehouse)

- Standardize data domains and analytics while protecting sensitive judicial data.
- Raw/Refined/Curated layers; open table formats (Iceberg/Delta/Hudi); catalogs per cloud.
- CDC/ETL/ELT with DQ checks; lineage via OpenLineage; MDM golden records; tokenization and encryption.
- Reference architecture; data contracts; data product SLAs; stewardship model; onboarding SOP.
- DQ pass rate ≥ 99%; lineage present for tier-1 datasets; access requests within SLA.
- Raw/Refined/Curated layers; Iceberg/Delta/Hudi; catalog (Glue/Purview/Dataplex/OCI).
- CDC/ETL/ELT pipelines; DQ checks; lineage; MDM golden records; tokenization.
- Deliverables: reference architecture; data contracts; data product SLAs.
- Acceptance: DQ pass rate ≥ 99%; lineage present for tier-1 datasets.

9.3 Data Categorization & Tagging (Policy & Enforcement)

Adopt a unified classification model (**PII, PHI, CJIS, CUI, Public**) and enforce tagging across all cloud environments using standard metadata keys:
court_id, env, owner, data_class, cost_center, system, dr_tier, slo.

Policy-as-Code enforces tag presence and lineage completeness, denying create or update actions on chargeable or sensitive resources if required tags are missing. Lineage tracking is mandatory for Tier-1 datasets.

Policy Element	Definition	Enforcement
Classification Levels	PII, PHI, CJIS, CUI, Public	Catalog and automated policy checks
Required Tags	court_id, env, owner, data_class, cost_center, system, dr_tier, slo	Deny create/update if required tags are missing
Lineage	Tier-1 datasets must maintain complete lineage records	Data catalog integration with DQ and lineage jobs
Access	RBAC/ABAC with tokenization for sensitive data	IAM policies and data-layer enforcement

Acceptance: Tag compliance ≥ 95%; Tier-1 dataset lineage fully traceable; automated enforcement validated via quarterly policy scans.

10. Application Platforms

- Provide hardened platforms (K8s, PaaS, serverless) with provenance-verified delivery.
- Private clusters/registries; policy enforcement (OPA/Kyverno); autoscaling; blue/green and canary patterns.
- EKS/AKS/GKE/OKE add-on baselines; gateway/ingress; CSI/CNI; SLOs and golden pipelines; platform APIs.
- Cluster blueprints; platform SLOs; golden pipelines; multi-tenant isolation guide.
- Pod MTTR < 5m; provenance verified; error budgets respected.
- K8s (EKS/AKS/GKE/OKE) with baseline add-ons (Ingress, CSI, CNI, policy, autoscaling).
- Serverless + managed PaaS for rapid delivery; private registries; artifact signing.
- Deliverables: cluster blueprints; platform SLOs; golden pipelines; platform APIs.
- Acceptance: blue/green + canary proven; pod MTTR < 5m; provenance verified.

11. DevSecOps & Software Supply Chain

- Assure integrity of code and infra with policy gates and end-to-end provenance.
- CI/CD with OIDC; SAST/SCA/DAST/IAST; secrets scanning; exception workflow.
- SBOM/MLSBOM; SLSA level targets; Cosign/Sigstore attestations; artifact retention; reproducible builds.
- Pipeline-as-code templates; policy bundles; scan baselines; exception register; incident playbook.
- Zero critical vulns at release; signed provenance required for production deploys.
- CI/CD with OIDC; IaC policy gates (OPA/Rego); SAST/SCA/DAST/IAST; SARIF reporting.
- SBOM/MLSBOM; SLSA level targets; Cosign/Sigstore attestation; provenance enforcement.
- Deliverables: pipeline-as-code; policy bundles; waiver workflow; artifact retention.
- Acceptance: 0 critical vulns in release; provenance required for deploy.

Checklist Item	Status (☐/☑)	Evidence/Link	Owner
Provenance required for deploy; unsigned artifacts blocked	☐		Platform
SBOM/MLSBOM generated; Cosign/Sigstore attestations	☐		DevSecOps
SAST/SCA/DAST/IAST integrated; SARIF stored	☐		DevSecOps
OPA/Rego/Kyverno policy gates enforced	☐		DevSecOps
OIDC workload identity; no long-lived keys	☐		DevSecOps

Create golden pipelines with OIDC-based cloud auth, secrets-free runners, security gates, SBOM/MLSBOM, and signed provenance enforced at deploy.

11.4 CI/CD Pipelines (Provenance, SBOM, Policy Gates)

Establish standardized **pipeline-as-code frameworks** that ensure every artifact deployed to any court environment is verified, attested, and policy-compliant. Pipelines must integrate with the CCoE's central DevSecOps service catalog and conform to **SLSA Level 3+** supply-chain assurance.
Objectives
- Eliminate long-lived credentials through **OIDC-based workload identity**.

- Enforce **Policy-as-Code gates** using OPA /Rego and Kyverno for Kubernetes deployments.
- Mandate **SBOM / MLSBOM** generation, signing, and verification at every build.
- Require **signed provenance** (Cosign / Sigstore) before promotion or deployment.
- Ensure traceability from commit → build → deploy → runtime through audit trails.

Pipeline Architecture

Stage	Controls	Tooling / Evidence
Source & Commit	Code signing required; branch protection; pre-commit scans (SAST / SCA).	GitHub / GitLab w/ GPG signatures; Dependabot; SonarQube reports.
Build	Ephemeral runners (no static credentials); SBOM creation; artifact hashing.	OIDC runners; Syft / Grype; Cosign signatures.
Test & Scan	DAST, IAST, container scan before promotion.	OWASP ZAP, Anchore, Trivy; SARIF reports.
Policy Gate	OPA /Rego and Kyverno check SLSA, license, and CIS benchmarks.	Policy bundles; compliance runbooks.
Deploy & Attest	Provenance required; unsigned or non-SBOM artifacts blocked.	Sigstore Rekor log; Attestation records.
Monitor & Feedback	Post-deployment scan; drift detection; runtime policy audit.	Anchore Enterprise; Falco; Defender for Cloud.

Policy & Enforcement
- **Zero-trust pipeline**: every stage authenticates via ephemeral OIDC tokens scoped to the workload, not the user.
- **Automated waiver workflow** with expiration dates for approved exceptions.
- **Audit integration**: pipeline logs exported to central SIEM for ConMon evidence.
- **Retention**: all artifacts, SBOMs, and attestations retained for 12 months post-release.

Acceptance Criteria
- 100 % of deployable artifacts carry verifiable provenance and SBOM.
- 0 critical vulnerabilities in release.
- Policy gates enforced across all environments.
- All pipeline runs traceable to CCoE audit records.

12. AI/ML Foundations & Guardrails
- Enable safe, compliant AI/ML with strong governance and MLOps.
- AI RMF adoption; PPR guardrails; model cards/datasheets; evaluation harness with thresholds.
- Registry; feature stores; drift monitoring; rollback; KMS-integrated secrets; reproducible pipelines.
- Model governance plan; dataset SOPs; audit trail patterns; secure training/serving blueprints.
- Eval thresholds met; drift alerts wired; red-team exercises completed.
- AI RMF; PPR guardrails; model documentation; evaluation harness; bias testing.
- MLOps: registry; features; drift monitoring; rollback plans; secret mgmt via KMS.
- Deliverables: model governance plan; dataset handling SOPs; audit trails.
- Acceptance: eval thresholds met; drift alerts wired; red-teaming completed.

13. Operations: ITSM + SRE + DR/BCP
- Run with discipline: CAB/ECAB, SoD, CMDB/SACM, ICS, DR/BCP validated.

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

- Runbook library; tabletop calendar; backup & recovery tests; RFO template; scorecards.
- Incident Command System; blameless postmortems with CAPA; service maps; quarterly DR tests.
- Runbooks; ICS roles; DR playbooks; operations scorecard.
- MTTD/MTTR within targets; DR tests pass; corrective actions implemented.
- Change mgmt via CAB/ECAB; SoD; CMDB/SACM; KEDB; incident command system.
- Runbooks library; tabletop exercises; DR playbooks; backup & recovery tests.
- Deliverables: service maps; RFO template; operations scorecard.
- Acceptance: quarterly DR tests pass; MTTD/MTTR within target bands.

14. FinOps & Cost Governance

- Cost transparency and optimization across 300 courts.
- CUR/billing exports; budgets/alerts; anomaly detection; unit economics (TACoS).
- Discount mgmt (SP/RI/CUD/SUD); rightsizing; license optimization; tag compliance audits; COA mapping.
- Dashboards; optimization backlog with savings estimates; chargeback/showback model; tagging standards.
- ≥ 20% savings vs baseline; ±5% budget adherence; 100% tag compliance on chargeable resources.
- CUR/billing exports; budgets & alerts; anomaly detection; unit economics (TACoS).
- Discount mgmt: SP/RI/CUD/SUD; rightsizing; license optimization; COA mapping.
- Deliverables: dashboards; optimization backlog; chargeback/showback model.
- Acceptance: ≥ 20% savings over baseline; budget adherence within ±5%.

15. Migration Factory (Court Waves)

- Move at scale with readiness gates and zero P1 at go-live.
- Discovery inventories; dependency maps; data classification; parity checks; remediation tracks.
- H2H/E2E migration runbooks; SIT/UAT gates; CTO with rollback; hypercare; PIR with CAPA.
- Wave plan; per-court dossier; acceptance criteria; KPI/OKR set; comms plan; blackout windows.
- 0 P1 incidents at go-live; 100% reconciliation; performance within SLOs; sign-offs complete.
- Readiness: inventories, dependencies, data mapping, environment parity checks.
- Execution: H2H/E2E, SIT/UAT; cutover (CTO) with rollback; post-cutover PIR.
- Deliverables: wave plan; per-court dossier; acceptance criteria; KPI/OKR set.
- Acceptance: zero P1 sev incidents at go-live; data reconciliation 100%.

16. Training, Readiness, and Change Management

- Upskill courts and CCoE for sustained operations.
- Role-based curricula; ILT/VILT; hands-on labs; T3 enablement; sandbox environments.
- LMS-integrated content; knowledge checks; office hours; certification paths; adoption KPIs.
- Curriculum; lab guides; knowledge checks; comms plan; certification maps.
- ≥95% completion; ≥80% proficiency; adoption KPIs on track; feedback loop established.
- Role-based curricula; ILT/VILT; labs; T3 enablement; adoption KPIs.
- Security handling IL5/IL6-like for training data; sandboxed environments.

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Page 32 of 117

- Deliverables: curriculum, lab guides, knowledge checks, comms plan.
- Acceptance: completion ≥ 95%; proficiency ≥ 80% on assessments.

17. Roadmap & Phases (12–18 Months)

- Stage delivery over 18 months with compliance/cost gates.
- Phase gates based on compliance, availability, and cost variance thresholds; monthly executive reviews.
- Phase 0–4 with named outcomes; staffing/resourcing matrices aligned to wave cadence.
- Integrated Master Schedule; resource plan; phase exit checklists; risk register cadence.
- All gates passed per phase; risks tracked; cost variance within ±5%; stakeholder sign-off.
- Phase 0 (M0–1): CCoE stand-up; charter; RACI; SOPs; discovery.
- Phase 1 (M1–3): LZ MVPs; identity/network/security baselines; circuits.
- Phase 2 (M3–6): Data platform; DevSecOps; observability; FinOps dashboards.
- Phase 3 (M6–12): App platform GA; AI/ML guardrails; first 50 courts.
- Phase 4 (M12–18): Scale to 300 courts; ATOs; optimization & de-risking.

18. Risks and RAID Log

ID	Risk	Impact	Likelihood	Mitigation	Owner
R-01	Court data classification gaps	High	Med	Enforce PTA/PIA, DLP, catalog lineage	CISO
R-02	Cross-cloud identity drift	Med	Med	Central IdP, SCIM/JIT, policy as code	Identity Lead
R-03	Cost overruns	Med	Med	Commit discounts, anomaly guardrails, unit economics	FinOps
R-04	Circuit delays (DX/ER/Interconnect/FastConnect)	High	Med	Expedite orders; temporary VPN; bandwidth shaping	Network
R-05	Tool sprawl across courts	Med	High	Standardize toolchain; golden images; training	CCoE
R-06	Key management inconsistency	High	Low	Central KMS patterns; rotation; BYOK/HYOK policy	Security
R-07	Insufficient test coverage pre-cutover	High	Med	Gateways with SIT/UAT exit criteria; dry runs	QA Lead
R-08	Sovereignty constraints block analytics	Med	Low	Use VPC-SC/data perimeters; localized processing	Data
R-09	Vendor lock-in	Med	Med	Abstraction via contracts, IaC, portability patterns	EA
R-10	Workforce readiness	Med	Med	T3; role-based pathways; labs; shadowing	Training
R-11	Inadequate tagging impacts FinOps	Med	High	Mandatory tagging policy; budget alerts; audits	FinOps
R-12	Privileged access misuse	High	Low	PAW; JIT/JEA; PAM; session recording	Security

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Page 33 of 117

R-13	Incident response immaturity	Med	Med	Runbooks; tabletops; KEDB; on-call rotations	SRE
R-14	Supply chain integrity gaps	High	Low	SBOM/SLSA; provenance; policy gates	DevSecOps
R-15	Data quality regressions	Med	Med	DQ SLAs; lineage; canary checks; rollback	Data
R-16	Scope creep	Med	Med	ARB for scope changes; change budget; ADRs	PMO
R-17	Regulatory changes	Med	Low	Compliance watch; update control narratives	Compliance
R-18	Third-party outages	High	Med	Multi-region/DR; failover contracts; runbooks	SRE
R-19	Court-specific exceptions multiply	Med	Med	Exception registry; timeboxed waivers; sunset dates	CCoE
R-20	Knowledge siloing	Med	High	Docs-as-code; internal portal; communities of practice	CCoE

Aligned to the structure used in the Court System Hybrid Multi-Cloud Integration package; extended to add 300 courts and a centralized CCoE.

ID	Objective	Measure of Success (MoS)	Target/Date
O1	Stand up compliant landing zones in AWS/Azure/GCP/OCI	Policy compliance; conformance pack; drift-free baseline	≥98% policies green by M3 (MVP)
O2	Private access to PaaS services in all clouds	No public egress for PaaS; endpoint coverage	100% critical services via PE/PL/PSC/SG by M4
O3	Establish CCoE governance with ARB/CCB/ECAB	SOPs approved; RFC lead time; PIR completion	SOPs signed M1; RFC→PIR cycle < 14 days
O4	Data platform (lakehouse) with catalog & DQ SLAs	DQ pass rate; lineage coverage	≥99% DQ; lineage for Tier-1 datasets by M6
O5	DevSecOps pipelines with SLSA-aligned integrity	Provenance required; SBOM coverage; gate pass rate	100% deploys with provenance by M6
O6	ITSM+SRE with tested DR/BCP	DR test pass; MTTD/MTTR	Quarterly DR pass; MTTR < 30m P1
O7	Migrate courts via repeatable waves	Readiness gates; zero P1 at go-live	50 courts by M12; 300 by M18

Domain	Acceptance Criteria
Landing zones	≥98% policy compliance; conformance pack green; drift checks scheduled.
Identity	Break-glass tested; no standing privileged accounts; quarterly access reviews complete.
Networking	Private access enforced for critical PaaS; HA failover < 60s in tests.
Security	Control narratives approved; FIPS 140-3 KMS policies; STIG/CIS scans passed.
Observability	Detections-as-code live; dashboards published; alert runbooks game-day validated.
Data	DQ SLAs met; Tier-1 lineage; RBAC/ABAC policies enforced.
DevSecOps	Signed provenance required; SBOM 100%; critical vulns blocked.
Operations	SOP library published; DR/BCP exercises passed.
Migration	Readiness gate signed; zero P1 at go-live; reconciliation 100%.

Milestone	Target Date	Exit Criteria
M0: Program kickoff & CCoE charter	M0+2w	Charter/RACI/SOPs approved
M1: LZ MVP (all clouds)	M1	Baseline identity/network/security; policy ≥ 90%
M3: Private access to PaaS	M3	Critical services via PE/PL/PSC/SG; no public exposure
M6: Data platform foundation & DevSecOps	M6	DQ ≥99%; provenance enforced; dashboards live
M9: App platform GA	M9	EKS/AKS/GKE/OKE baseline GA; blue/green proven
M12: 50 courts migrated	M12	Zero P1 at go-live; reconciliation 100%
M18: 300 courts migrated	M18	All waves complete; optimization backlog running

Objective	Description	Success Criteria	Priority
Enhance Availability	Increase uptime via DR/HA	99.99% uptime achieved	High
Improve Security Posture	Apply Zero Trust and IL5 controls	All workloads pass STIG scans	High
Enable Scalability	Scale during peak operations	Resource utilization < 75% at peak	Medium
Reduce Operational Costs	Rightsize, commit discounts	20% savings over 12 months	Medium
Improve Data Access	Secure remote access	Role-based access tested	High
Support Multicloud Resilience	Cross-cloud DR	DR plan tested	Low

Document Title	Description	Required Format
System Security Plan (SSP)	Architecture, boundaries, controls; include ingress/egress details	DOCX / XML
Network Topology Diagrams	DMZ, ingress/egress, security stack, cloud links	VSDX / PDF
Security Control Traceability Matrix (SCTM)	RMF control→implementation mapping	XLSX
Boundary Definition Document	System boundary, IP ranges, subnets, interconnects	DOCX
PPSM	Approved ports/protocols with justifications	XLSX
Security Configuration Guides (SCGs)	Vendor hardening guides/STIGs applied	PDF/DOCX
Change Management Plan	Propose/test/approve/log changes process	DOCX
Incident Response Plan (IRP)	Detect/report/respond for perimeter events	DOCX
Continuous Monitoring Strategy	Logging, SIEM integration, cadence	DOCX
Configuration Management Plan	Versioning, backups, restoration, tracking	DOCX
System Interconnection Agreement (SIA/MOU)	External connections agreements	DOCX
Contingency Plan (CP)	Failover for gateways, redundant links	DOCX
Encryption Key Management Plan	TLS cert/key generation/rotation/storage	DOCX
Asset Inventory List	All perimeter devices with details	XLSX
STIG Compliance Checklist	Boundary system STIG reports	CKL/XLSX
Vulnerability Scan Results	Recent ACAS/Nessus scans (<30 days)	PDF
POA&M	Unresolved weaknesses and findings	XLSX
Risk Assessment Report (RAR)	Threat analysis and posture for boundary	DOCX
Penetration Test Reports	Red team or contracted tests	PDF
Data Flow Diagrams (DFD)	Ingress/egress flows, protocols, encryption	VSDX/PDF

Cloud	Dedicated Link	VPN Option
AWS GovCloud	Direct Connect	Site-to-Site VPN
Azure Government	ExpressRoute	Azure VPN Gateway
Google Cloud for Government	Partner/Dedicated Interconnect	Cloud VPN
Oracle NSR	FastConnect	IPSec VPN

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Role	Responsibility	
Cloud Operations Lead	Oversees multi-cloud ops and escalations	
Security Officer (ISSO/ISSM)	Cyber compliance and STIG application	
Network Engineer	Routing, firewalls, perimeter controls	
Cloud Systems Administrator	VM/container/platform operations	
DevSecOps Engineer	CI/CD pipelines, scanners, automation	
Compliance Manager	RMF/ATO evidence and document control	
Help Desk / Tier Support	First response, triage, comms	
Milestone	**Target Date**	**Exit Criteria**
M0: Program kickoff & CCoE charter	M0+2w	Charter/RACI/SOPs approved
M1: LZ MVP (all clouds)	M1	Baseline identity/network/security; policy ≥ 90%
M3: Private access to PaaS	M3	Critical services via PE/PL/PSC/SG; no public exposure
M6: Data platform foundation & DevSecOps	M6	DQ ≥99%; provenance enforced; dashboards live
M9: App platform GA	M9	EKS/AKS/GKE/OKE baseline GA; blue/green proven
M12: 50 courts migrated	M12	Zero P1 at go-live; reconciliation 100%
M18: 300 courts migrated	M18	All waves complete; optimization backlog running

APPENDICES

The following appendices provide court-ready checklists, templates, and catalogs to support wave planning, acceptance, and ATO evidence capture.

Appendix F — Court Wave Acceptance Checklists (Per-Cloud & Per-Domain)

Use these tables during wave readiness reviews. Status uses □/☑ with evidence links; sign-off captured per court.

F.A — Landing Zones & Guardrails

AWS GovCloud

Checklist Item	Status (□/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
Policies green ≥98% via AWS Config conformance packs + SCPs	□			
Court tenant unit created; tags: court_id, env, owner, data_class	□			
Central logging/monitoring account/project configured; immutable retention	□			
Key management (KMS/HSM) with rotation & separation of duties	□			
Network baseline hub-spoke; egress controls; DNS via Route 53 Resolver	□			
Private access to PaaS via PrivateLink	□			
Break-glass access tested; audit immutability verified	□			

Court Representative (Name/Title/Signature/Date): _____

Azure Government

Checklist Item	Status (□/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
Policies green ≥98% via Azure Policy/Initiatives @ MG	□			

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Page 38 of 117

Court tenant unit created; tags: court_id, env, owner, data_class	☐			
Central logging/monitoring account/project configured; immutable retention	☐			
Key management (KMS/HSM) with rotation & separation of duties	☐			
Network baseline hub-spoke; egress controls; DNS via Azure DNS / Private Resolver	☐			
Private access to PaaS via Private Link	☐			
Break-glass access tested; audit immutability verified	☐			

Court Representative (Name/Title/Signature/Date): _____

Google Cloud for Government

Checklist Item	Status (☐/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
Policies green ≥98% via Org Policy constraints + scanners	☐			
Court tenant unit created; tags: court_id, env, owner, data_class	☐			
Central logging/monitoring account/project configured; immutable retention	☐			
Key management (KMS/HSM) with rotation & separation of duties	☐			
Network baseline hub-spoke; egress	☐			

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Page 39 of 117

Checklist Item	Status (□/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
controls; DNS via Cloud DNS + Private DNS				
Private access to PaaS via Private Service Connect	□			
Break-glass access tested; audit immutability verified	□			

Court Representative (Name/Title/Signature/Date): _____

Oracle NSR

Checklist Item	Status (□/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
Policies green ≥98% via Security Zones + IAM policies	□			
Court tenant unit created; tags: court_id, env, owner, data_class	□			
Central logging/monitoring account/project configured; immutable retention	□			
Key management (KMS/HSM) with rotation & separation of duties	□			
Network baseline hub-spoke; egress controls; DNS via OCI DNS + Resolver	□			
Private access to PaaS via Service Gateway	□			
Break-glass access tested; audit immutability verified	□			

Court Representative (Name/Title/Signature/Date): _____

F.B — Identity & Access

AWS GovCloud

Checklist Item	Status (☐/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
Federation to IdP with CAC/PIV; MFA enforced for admins	☐			
Role catalog implemented; least privilege verified; JIT/JEA configured	☐			
PAM elevation with approvals; session recording enabled	☐			
Quarterly access review cadence established; immutable audit logs	☐			

Court Representative (Name/Title/Signature/Date): _____

Azure Government

Checklist Item	Status (☐/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
Federation to IdP with CAC/PIV; MFA enforced for admins	☐			
Role catalog implemented; least privilege verified; JIT/JEA configured	☐			
PAM elevation with approvals; session recording enabled	☐			
Quarterly access review cadence established; immutable audit logs	☐			

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Page 41 of 117

Court Representative (Name/Title/Signature/Date): _____

Google Cloud for Government

Checklist Item	Status (☐/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
Federation to IdP with CAC/PIV; MFA enforced for admins	☐			
Role catalog implemented; least privilege verified; JIT/JEA configured	☐			
PAM elevation with approvals; session recording enabled	☐			
Quarterly access review cadence established; immutable audit logs	☐			

Court Representative (Name/Title/Signature/Date): _____

Oracle NSR

Checklist Item	Status (☐/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
Federation to IdP with CAC/PIV; MFA enforced for admins	☐			
Role catalog implemented; least privilege verified; JIT/JEA configured	☐			
PAM elevation with approvals; session recording enabled	☐			
Quarterly access review cadence established; immutable audit logs	☐			

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Court Representative (Name/Title/Signature/Date): _____

F.C — Networking & Connectivity

AWS GovCloud

Checklist Item	Status (□/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
Non-overlapping IPAM; subnet plan approved	□			
Regional hub peered; routing and NAT configured	□			
Firewall/L7 policy sets applied; RPZ/response policies in place	□			
Private endpoints for registries/PaaS via PrivateLink	□			
Dedicated circuits live or VPN interim; HA tested <60s	□			
Validation: packet loss <0.1%; latency/bandwidth within SLOs	□			

Court Representative (Name/Title/Signature/Date): _____

Azure Government

Checklist Item	Status (□/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
Non-overlapping IPAM; subnet plan approved	□			
Regional hub peered; routing and NAT configured	□			
Firewall/L7 policy sets applied; RPZ/response policies in place	□			
Private endpoints for registries/PaaS via Private Link	□			
Dedicated circuits live or VPN interim; HA tested <60s	□			

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Page 43 of 117

Validation: packet loss <0.1%; latency/bandwidth within SLOs	☐			

Court Representative (Name/Title/Signature/Date): _____

Google Cloud for Government

Checklist Item	Status (☐/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
Non-overlapping IPAM; subnet plan approved	☐			
Regional hub peered; routing and NAT configured	☐			
Firewall/L7 policy sets applied; RPZ/response policies in place	☐			
Private endpoints for registries/PaaS via Private Service Connect	☐			
Dedicated circuits live or VPN interim; HA tested <60s	☐			
Validation: packet loss <0.1%; latency/bandwidth within SLOs	☐			

Court Representative (Name/Title/Signature/Date): _____

Oracle NSR

Checklist Item	Status (☐/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
Non-overlapping IPAM; subnet plan approved	☐			
Regional hub peered; routing and NAT configured	☐			
Firewall/L7 policy sets applied; RPZ/response policies in place	☐			

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Page 44 of 117

Private endpoints for registries/PaaS via Service Gateway	☐			
Dedicated circuits live or VPN interim; HA tested <60s	☐			
Validation: packet loss <0.1%; latency/bandwidth within SLOs	☐			

Court Representative (Name/Title/Signature/Date): _____

F.D — Security, RMF/ATO

AWS GovCloud

Checklist Item	Status (☐/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
FIPS 140-3 crypto enforced; key lifecycles documented	☐			
STIG/CIS baselines applied; scans attached	☐			
Native detections enabled; CloudWatch/CloudTrail → SIEM; Security Hub; GuardDuty	☐			
IR playbooks tested (tabletop or live)	☐			
ConMon dashboards live; thresholds defined	☐			

Court Representative (Name/Title/Signature/Date): _____

Azure Government

Checklist Item	Status (☐/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
FIPS 140-3 crypto enforced; key lifecycles documented	☐			
STIG/CIS baselines applied; scans attached	☐			
Native detections enabled; Log Analytics → Microsoft	☐			

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Sentinel; Defender for Cloud				
IR playbooks tested (tabletop or live)	☐			
ConMon dashboards live; thresholds defined	☐			

Court Representative (Name/Title/Signature/Date): _____

Google Cloud for Government

Checklist Item	Status (☐/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
FIPS 140-3 crypto enforced; key lifecycles documented	☐			
STIG/CIS baselines applied; scans attached	☐			
Native detections enabled; Cloud Logging/Monitoring → SIEM; Security Command Center	☐			
IR playbooks tested (tabletop or live)	☐			
ConMon dashboards live; thresholds defined	☐			

Court Representative (Name/Title/Signature/Date): _____

Oracle NSR

Checklist Item	Status (☐/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
FIPS 140-3 crypto enforced; key lifecycles documented	☐			
STIG/CIS baselines applied; scans attached	☐			
Native detections enabled; Logging/Monitoring	☐			

→ SIEM; Cloud Guard				
IR playbooks tested (tabletop or live)	☐			
ConMon dashboards live; thresholds defined	☐			

Court Representative (Name/Title/Signature/Date): _____

F.E — Logging, Monitoring & Observability

AWS GovCloud

Checklist Item	Status (☐/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
Platform/network/security logs flowing to SIEM (CloudWatch/CloudTrail → SIEM; Security Hub; GuardDuty)	☐			
Dashboards: LZ, identity, network, app, data	☐			
Alert policy & on-call rota; noise reduction backlog	☐			
Synthetic probes for critical journeys	☐			
Top 20 detections validated	☐			

Court Representative (Name/Title/Signature/Date): _____

Azure Government

Checklist Item	Status (☐/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
Platform/network/security logs flowing to SIEM (Log Analytics → Microsoft Sentinel; Defender for Cloud)	☐			
Dashboards: LZ, identity, network, app, data	☐			
Alert policy & on-call rota; noise reduction backlog	☐			
Synthetic probes for critical journeys	☐			
Top 20 detections validated	☐			

Court Representative (Name/Title/Signature/Date): _____

Google Cloud for Government

Checklist Item	Status (☐/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Checklist Item	Status (□/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
Platform/network/security logs flowing to SIEM (Cloud Logging/Monitoring → SIEM; Security Command Center)	□			
Dashboards: LZ, identity, network, app, data	□			
Alert policy & on-call rota; noise reduction backlog	□			
Synthetic probes for critical journeys	□			
Top 20 detections validated	□			

Court Representative (Name/Title/Signature/Date): _____

Oracle NSR

Checklist Item	Status (□/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
Platform/network/security logs flowing to SIEM (Logging/Monitoring → SIEM; Cloud Guard)	□			
Dashboards: LZ, identity, network, app, data	□			
Alert policy & on-call rota; noise reduction backlog	□			
Synthetic probes for critical journeys	□			
Top 20 detections validated	□			

Court Representative (Name/Title/Signature/Date): _____

F.F — Data Platform (Lakehouse)

AWS GovCloud

Checklist Item	Status (□/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
Catalog registered (AWS Glue); domains onboarded	□			
Raw/Refined/Curated layers created; encryption default-on	□			
DQ checks automated; pass rate ≥99%	□			
Lineage captured for tier-1 datasets	□			
RBAC/ABAC policies; tokenization/pseudonymization applied	□			

Court Representative (Name/Title/Signature/Date): _____

Azure Government

Checklist Item	Status (□/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
Catalog registered (Microsoft Purview); domains onboarded	□			
Raw/Refined/Curated layers created; encryption default-on	□			
DQ checks automated; pass rate ≥99%	□			
Lineage captured for tier-1 datasets	□			
RBAC/ABAC policies; tokenization/pseudonymization applied	□			

Court Representative (Name/Title/Signature/Date): _____

Google Cloud for Government

Checklist Item	Status (□/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
Catalog registered (Dataplex + Data Catalog); domains onboarded	□			
Raw/Refined/Curated layers created; encryption default-on	□			
DQ checks automated; pass rate ≥99%	□			
Lineage captured for tier-1 datasets	□			
RBAC/ABAC policies; tokenization/pseudonymization applied	□			

Court Representative (Name/Title/Signature/Date): _____

Oracle NSR

Checklist Item	Status (□/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
Catalog registered (OCI Data Catalog); domains onboarded	□			
Raw/Refined/Curated layers created; encryption default-on	□			
DQ checks automated; pass rate ≥99%	□			
Lineage captured for tier-1 datasets	□			
RBAC/ABAC policies; tokenization/pseudonymization applied	□			

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Court Representative (Name/Title/Signature/Date): _____

F.G — Application Platforms (Kubernetes/Serverless)

AWS GovCloud

Checklist Item	Status (☐/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
Kubernetes baseline ready (EKS + ECR); private planes	☐			
Ingress/Gateway, CSI, CNI, policy, autoscaling installed	☐			
Private registries; signed images; provenance verification	☐			
Blue/green + canary validated; rollback tested	☐			
Platform SLOs & error budgets defined	☐			

Court Representative (Name/Title/Signature/Date): _____

Azure Government

Checklist Item	Status (☐/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
Kubernetes baseline ready (AKS + ACR); private planes	☐			
Ingress/Gateway, CSI, CNI, policy, autoscaling installed	☐			
Private registries; signed images; provenance verification	☐			
Blue/green + canary validated; rollback tested	☐			
Platform SLOs & error budgets defined	☐			

Court Representative (Name/Title/Signature/Date): _____

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Google Cloud for Government

Checklist Item	Status (☐/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
Kubernetes baseline ready (GKE + Artifact Registry); private planes	☐			
Ingress/Gateway, CSI, CNI, policy, autoscaling installed	☐			
Private registries; signed images; provenance verification	☐			
Blue/green + canary validated; rollback tested	☐			
Platform SLOs & error budgets defined	☐			

Court Representative (Name/Title/Signature/Date): _____

Oracle NSR

Checklist Item	Status (☐/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
Kubernetes baseline ready (OKE + OCIR); private planes	☐			
Ingress/Gateway, CSI, CNI, policy, autoscaling installed	☐			
Private registries; signed images; provenance verification	☐			
Blue/green + canary validated; rollback tested	☐			
Platform SLOs & error budgets defined	☐			

Court Representative (Name/Title/Signature/Date): _____

F.H — DevSecOps & Software Supply Chain

AWS GovCloud

Checklist Item	Status (☐/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
CI/CD with OIDC; secrets removed; least-privilege runners	☐			
OPA/Rego/Kyverno gates; quality gates defined	☐			
SAST/SCA/DAST/IAST with SARIF reporting	☐			
SBOM/MLSBOM generated; signed provenance required	☐			
Waiver/exception workflow with expiry	☐			

Court Representative (Name/Title/Signature/Date): _____

Azure Government

Checklist Item	Status (☐/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
CI/CD with OIDC; secrets removed; least-privilege runners	☐			
OPA/Rego/Kyverno gates; quality gates defined	☐			
SAST/SCA/DAST/IAST with SARIF reporting	☐			
SBOM/MLSBOM generated; signed provenance required	☐			
Waiver/exception workflow with expiry	☐			

Court Representative (Name/Title/Signature/Date): _____

Google Cloud for Government

Checklist Item	Status (☐/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
CI/CD with OIDC; secrets removed; least-privilege runners	☐			
OPA/Rego/Kyverno gates; quality gates defined	☐			

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Checklist Item	Status (□/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
SAST/SCA/DAST/IAST with SARIF reporting	□			
SBOM/MLSBOM generated; signed provenance required	□			
Waiver/exception workflow with expiry	□			

Court Representative (Name/Title/Signature/Date): _____

Oracle NSR

Checklist Item	Status (□/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
CI/CD with OIDC; secrets removed; least-privilege runners	□			
OPA/Rego/Kyverno gates; quality gates defined	□			
SAST/SCA/DAST/IAST with SARIF reporting	□			
SBOM/MLSBOM generated; signed provenance required	□			
Waiver/exception workflow with expiry	□			

Court Representative (Name/Title/Signature/Date): _____

F.I — Operations: ITSM + SRE + DR/BCP

AWS GovCloud

Checklist Item	Status (□/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
SOP library published; ICS roles assigned	□			
Change mgmt (CAB/ECAB) operational; SoD enforced	□			
Service maps/CMDB updated for court workloads	□			
Backup/restore tests passed; DR playbook executed	□			

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Page 54 of 117

Checklist Item	Status (☐/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
MTTD/MTTR targets met (drills)	☐			

Court Representative (Name/Title/Signature/Date): _____

Azure Government

Checklist Item	Status (☐/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
SOP library published; ICS roles assigned	☐			
Change mgmt (CAB/ECAB) operational; SoD enforced	☐			
Service maps/CMDB updated for court workloads	☐			
Backup/restore tests passed; DR playbook executed	☐			
MTTD/MTTR targets met (drills)	☐			

Court Representative (Name/Title/Signature/Date): _____

Google Cloud for Government

Checklist Item	Status (☐/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
SOP library published; ICS roles assigned	☐			
Change mgmt (CAB/ECAB) operational; SoD enforced	☐			
Service maps/CMDB updated for court workloads	☐			
Backup/restore tests passed; DR playbook executed	☐			

Checklist Item	Status (□/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
MTTD/MTTR targets met (drills)	□			

Court Representative (Name/Title/Signature/Date): _____

Oracle NSR

Checklist Item	Status (□/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
SOP library published; ICS roles assigned	□			
Change mgmt (CAB/ECAB) operational; SoD enforced	□			
Service maps/CMDB updated for court workloads	□			
Backup/restore tests passed; DR playbook executed	□			
MTTD/MTTR targets met (drills)	□			

Court Representative (Name/Title/Signature/Date): _____

F.J — FinOps & Cost Governance

AWS GovCloud

Checklist Item	Status (□/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
Billing export configured (AWS Cost & Usage Report (CUR) → S3)	□			
Budgets & alerts per court; anomaly detection live	□			
SP/RI/CUD/SUD instruments applied	□			
Tag compliance ≥95% on	□			

Checklist Item	Status (☐/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
chargeable resources				
Monthly variance within ±5%	☐			

Court Representative (Name/Title/Signature/Date): _____

Azure Government

Checklist Item	Status (☐/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
Billing export configured (Azure Cost Management export)	☐			
Budgets & alerts per court; anomaly detection live	☐			
SP/RI/CUD/SUD instruments applied	☐			
Tag compliance ≥95% on chargeable resources	☐			
Monthly variance within ±5%	☐			

Court Representative (Name/Title/Signature/Date): _____

Google Cloud for Government

Checklist Item	Status (☐/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
Billing export configured (Billing Export → BigQuery/Files)	☐			
Budgets & alerts per court; anomaly detection live	☐			
SP/RI/CUD/SUD instruments applied	☐			
Tag compliance ≥95% on chargeable resources	☐			

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Page 57 of 117

Checklist Item	Status (□/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
Monthly variance within ±5%	□			

Court Representative (Name/Title/Signature/Date): _____

Oracle NSR

Checklist Item	Status (□/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
Billing export configured (Cost & Usage Reports → Object Storage)	□			
Budgets & alerts per court; anomaly detection live	□			
SP/RI/CUD/SUD instruments applied	□			
Tag compliance ≥95% on chargeable resources	□			
Monthly variance within ±5%	□			

Court Representative (Name/Title/Signature/Date): _____

F.K — Migration Factory (Court Waves)

AWS GovCloud

Checklist Item	Status (□/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
Court dossier complete; dependencies & data map verified	□			
Readiness gate passed; SIT/UAT plans ready	□			
Cutover runbook approved; rollback path verified	□			
Hypercare staffed; comms plan issued	□			
PIR completed with CAPA	□			

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Court Representative (Name/Title/Signature/Date): _____

Azure Government

Checklist Item	Status (☐/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
Court dossier complete; dependencies & data map verified	☐			
Readiness gate passed; SIT/UAT plans ready	☐			
Cutover runbook approved; rollback path verified	☐			
Hypercare staffed; comms plan issued	☐			
PIR completed with CAPA	☐			

Court Representative (Name/Title/Signature/Date): _____

Google Cloud for Government

Checklist Item	Status (☐/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
Court dossier complete; dependencies & data map verified	☐			
Readiness gate passed; SIT/UAT plans ready	☐			
Cutover runbook approved; rollback path verified	☐			
Hypercare staffed; comms plan issued	☐			
PIR completed with CAPA	☐			

Court Representative (Name/Title/Signature/Date): _____

Oracle NSR

Checklist Item	Status (☐/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Page 59 of 117

Checklist Item	Status (☐/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
Court dossier complete; dependencies & data map verified	☐			
Readiness gate passed; SIT/UAT plans ready	☐			
Cutover runbook approved; rollback path verified	☐			
Hypercare staffed; comms plan issued	☐			
PIR completed with CAPA	☐			

Court Representative (Name/Title/Signature/Date): _____

F.L — Training, Readiness & Change Management

AWS GovCloud

Checklist Item	Status (☐/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
Role-based curricula delivered (IT, security, data, platform)	☐			
Completion ≥95% and proficiency ≥80%	☐			
Lab guides & sandbox access provisioned	☐			
Office hours and feedback loop active	☐			

Court Representative (Name/Title/Signature/Date): _____

Azure Government

Checklist Item	Status (☐/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
Role-based curricula delivered (IT, security, data, platform)	☐			

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Page 60 of 117

Checklist Item	Status (□/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
Completion ≥95% and proficiency ≥80%	□			
Lab guides & sandbox access provisioned	□			
Office hours and feedback loop active	□			

Court Representative (Name/Title/Signature/Date): _____

Google Cloud for Government

Checklist Item	Status (□/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
Role-based curricula delivered (IT, security, data, platform)	□			
Completion ≥95% and proficiency ≥80%	□			
Lab guides & sandbox access provisioned	□			
Office hours and feedback loop active	□			

Court Representative (Name/Title/Signature/Date): _____

Oracle NSR

Checklist Item	Status (□/☑)	Evidence / Link	Court Sign-off (Name/Date)	Notes
Role-based curricula delivered (IT, security, data, platform)	□			
Completion ≥95% and proficiency ≥80%	□			
Lab guides & sandbox access provisioned	□			

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Page 61 of 117

Office hours and feedback loop active	☐			

Court Representative (Name/Title/Signature/Date): _____

Appendix G — Court Dossier & Readiness Gate Templates

Duplicate this packet per court. Use Wave tabs (W1–W10) to track execution and acceptance.

G.1 Court Dossier Template

Field	Value/Notes
Court ID	
Environment	DEV / TEST / PROD
Primary Contacts	Name, role, email, phone
Data Classes	PII / PHI / CJIS / CUI / other
Target Cloud(s)	AWS / Azure / GCP / OCI
Dependencies	Systems, databases, external APIs
Availability/SLO	e.g., 99.9%
Change Windows	Approved cutover windows
Security Exceptions	List any waivers/POA&M items
Notes	

G.2 Wave Readiness Gate

Gate Item	Status (□/☑)	Evidence	Owner	Due Date
Discovery inventory complete; dependency map validated	□			
Data classification & tagging applied	□			
Landing zone controls green; private access enforced	□			
Connectivity validated; HA tested	□			
Security scans passed; exceptions documented	□			
Cutover plan approved; rollback tested	□			
UAT sign-off received	□			

G.3 Wave 1 — Court Sign-off Sheet

Domain	Cloud	Checklist Complete (☐/☑)	Evidence Link	Approver (Name/Date)
A Landing Zones & Guardrails	AWS GovCloud	☐		
A Landing Zones & Guardrails	Azure Government	☐		
A Landing Zones & Guardrails	Google Cloud for Government	☐		
A Landing Zones & Guardrails	Oracle NSR	☐		
B Identity & Access	AWS GovCloud	☐		
B Identity & Access	Azure Government	☐		
B Identity & Access	Google Cloud for Government	☐		
B Identity & Access	Oracle NSR	☐		
C Networking & Connectivity	AWS GovCloud	☐		
C Networking & Connectivity	Azure Government	☐		
C Networking & Connectivity	Google Cloud for Government	☐		
C Networking & Connectivity	Oracle NSR	☐		
D Security, RMF/ATO	AWS GovCloud	☐		
D Security, RMF/ATO	Azure Government	☐		
D Security, RMF/ATO	Google Cloud for Government	☐		
D Security, RMF/ATO	Oracle NSR	☐		
E Logging, Monitoring & Observability	AWS GovCloud	☐		
E Logging, Monitoring & Observability	Azure Government	☐		
E Logging, Monitoring & Observability	Google Cloud for Government	☐		
E Logging, Monitoring & Observability	Oracle NSR	☐		
F Data Platform (Lakehouse)	AWS GovCloud	☐		
F Data Platform (Lakehouse)	Azure Government	☐		
F Data Platform (Lakehouse)	Google Cloud for Government	☐		

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

F Data Platform (Lakehouse)	Oracle NSR	☐		
G Application Platforms (Kubernetes/Serverless)	AWS GovCloud	☐		
G Application Platforms (Kubernetes/Serverless)	Azure Government	☐		
G Application Platforms (Kubernetes/Serverless)	Google Cloud for Government	☐		
G Application Platforms (Kubernetes/Serverless)	Oracle NSR	☐		
H DevSecOps & Software Supply Chain	AWS GovCloud	☐		
H DevSecOps & Software Supply Chain	Azure Government	☐		
H DevSecOps & Software Supply Chain	Google Cloud for Government	☐		
H DevSecOps & Software Supply Chain	Oracle NSR	☐		
I Operations: ITSM + SRE + DR/BCP	AWS GovCloud	☐		
I Operations: ITSM + SRE + DR/BCP	Azure Government	☐		
I Operations: ITSM + SRE + DR/BCP	Google Cloud for Government	☐		
I Operations: ITSM + SRE + DR/BCP	Oracle NSR	☐		
J FinOps & Cost Governance	AWS GovCloud	☐		
J FinOps & Cost Governance	Azure Government	☐		
J FinOps & Cost Governance	Google Cloud for Government	☐		
J FinOps & Cost Governance	Oracle NSR	☐		
K Migration Factory (Court Waves)	AWS GovCloud	☐		
K Migration Factory (Court Waves)	Azure Government	☐		
K Migration Factory (Court Waves)	Google Cloud for Government	☐		
K Migration Factory (Court Waves)	Oracle NSR	☐		
L Training, Readiness & Change Management	AWS GovCloud	☐		
L Training, Readiness & Change Management	Azure Government	☐		

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Domain	Cloud	Checklist Complete		
L Training, Readiness & Change Management	Google Cloud for Government	☐		
L Training, Readiness & Change Management	Oracle NSR	☐		

Court Executive Signature: _____ Date: _____

Migration Lead Signature: _____ Date: _____

G.3 Wave 2 — Court Sign-off Sheet

Domain	Cloud	Checklist Complete (☐/☑)	Evidence Link	Approver (Name/Date)
A Landing Zones & Guardrails	AWS GovCloud	☐		
A Landing Zones & Guardrails	Azure Government	☐		
A Landing Zones & Guardrails	Google Cloud for Government	☐		
A Landing Zones & Guardrails	Oracle NSR	☐		
B Identity & Access	AWS GovCloud	☐		
B Identity & Access	Azure Government	☐		
B Identity & Access	Google Cloud for Government	☐		
B Identity & Access	Oracle NSR	☐		
C Networking & Connectivity	AWS GovCloud	☐		
C Networking & Connectivity	Azure Government	☐		
C Networking & Connectivity	Google Cloud for Government	☐		
C Networking & Connectivity	Oracle NSR	☐		
D Security, RMF/ATO	AWS GovCloud	☐		
D Security, RMF/ATO	Azure Government	☐		
D Security, RMF/ATO	Google Cloud for Government	☐		
D Security, RMF/ATO	Oracle NSR	☐		
E Logging, Monitoring & Observability	AWS GovCloud	☐		
E Logging, Monitoring & Observability	Azure Government	☐		
E Logging, Monitoring & Observability	Google Cloud for Government	☐		

E Logging, Monitoring & Observability	Oracle NSR	☐		
F Data Platform (Lakehouse)	AWS GovCloud	☐		
F Data Platform (Lakehouse)	Azure Government	☐		
F Data Platform (Lakehouse)	Google Cloud for Government	☐		
F Data Platform (Lakehouse)	Oracle NSR	☐		
G Application Platforms (Kubernetes/Serverless)	AWS GovCloud	☐		
G Application Platforms (Kubernetes/Serverless)	Azure Government	☐		
G Application Platforms (Kubernetes/Serverless)	Google Cloud for Government	☐		
G Application Platforms (Kubernetes/Serverless)	Oracle NSR	☐		
H DevSecOps & Software Supply Chain	AWS GovCloud	☐		
H DevSecOps & Software Supply Chain	Azure Government	☐		
H DevSecOps & Software Supply Chain	Google Cloud for Government	☐		
H DevSecOps & Software Supply Chain	Oracle NSR	☐		
I Operations: ITSM + SRE + DR/BCP	AWS GovCloud	☐		
I Operations: ITSM + SRE + DR/BCP	Azure Government	☐		
I Operations: ITSM + SRE + DR/BCP	Google Cloud for Government	☐		
I Operations: ITSM + SRE + DR/BCP	Oracle NSR	☐		
J FinOps & Cost Governance	AWS GovCloud	☐		
J FinOps & Cost Governance	Azure Government	☐		
J FinOps & Cost Governance	Google Cloud for Government	☐		
J FinOps & Cost Governance	Oracle NSR	☐		
K Migration Factory (Court Waves)	AWS GovCloud	☐		
K Migration Factory (Court Waves)	Azure Government	☐		

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Domain	Cloud	Checklist Complete (☐/☑)		
K Migration Factory (Court Waves)	Google Cloud for Government	☐		
K Migration Factory (Court Waves)	Oracle NSR	☐		
L Training, Readiness & Change Management	AWS GovCloud	☐		
L Training, Readiness & Change Management	Azure Government	☐		
L Training, Readiness & Change Management	Google Cloud for Government	☐		
L Training, Readiness & Change Management	Oracle NSR	☐		

Court Executive Signature: _____ Date: _____

Migration Lead Signature: _____ Date: _____

G.3 Wave 3 — Court Sign-off Sheet

Domain	Cloud	Checklist Complete (☐/☑)	Evidence Link	Approver (Name/Date)
A Landing Zones & Guardrails	AWS GovCloud	☐		
A Landing Zones & Guardrails	Azure Government	☐		
A Landing Zones & Guardrails	Google Cloud for Government	☐		
A Landing Zones & Guardrails	Oracle NSR	☐		
B Identity & Access	AWS GovCloud	☐		
B Identity & Access	Azure Government	☐		
B Identity & Access	Google Cloud for Government	☐		
B Identity & Access	Oracle NSR	☐		
C Networking & Connectivity	AWS GovCloud	☐		
C Networking & Connectivity	Azure Government	☐		
C Networking & Connectivity	Google Cloud for Government	☐		
C Networking & Connectivity	Oracle NSR	☐		
D Security, RMF/ATO	AWS GovCloud	☐		
D Security, RMF/ATO	Azure Government	☐		
D Security, RMF/ATO	Google Cloud for Government	☐		

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

D Security, RMF/ATO	Oracle NSR	☐		
E Logging, Monitoring & Observability	AWS GovCloud	☐		
E Logging, Monitoring & Observability	Azure Government	☐		
E Logging, Monitoring & Observability	Google Cloud for Government	☐		
E Logging, Monitoring & Observability	Oracle NSR	☐		
F Data Platform (Lakehouse)	AWS GovCloud	☐		
F Data Platform (Lakehouse)	Azure Government	☐		
F Data Platform (Lakehouse)	Google Cloud for Government	☐		
F Data Platform (Lakehouse)	Oracle NSR	☐		
G Application Platforms (Kubernetes/Serverless)	AWS GovCloud	☐		
G Application Platforms (Kubernetes/Serverless)	Azure Government	☐		
G Application Platforms (Kubernetes/Serverless)	Google Cloud for Government	☐		
G Application Platforms (Kubernetes/Serverless)	Oracle NSR	☐		
H DevSecOps & Software Supply Chain	AWS GovCloud	☐		
H DevSecOps & Software Supply Chain	Azure Government	☐		
H DevSecOps & Software Supply Chain	Google Cloud for Government	☐		
H DevSecOps & Software Supply Chain	Oracle NSR	☐		
I Operations: ITSM + SRE + DR/BCP	AWS GovCloud	☐		
I Operations: ITSM + SRE + DR/BCP	Azure Government	☐		
I Operations: ITSM + SRE + DR/BCP	Google Cloud for Government	☐		
I Operations: ITSM + SRE + DR/BCP	Oracle NSR	☐		
J FinOps & Cost Governance	AWS GovCloud	☐		
J FinOps & Cost Governance	Azure Government	☐		
J FinOps & Cost Governance	Google Cloud for Government	☐		

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Domain	Cloud	Checklist Complete (□/☑)	Evidence Link	Approver (Name/Date)
J FinOps & Cost Governance	Oracle NSR	□		
K Migration Factory (Court Waves)	AWS GovCloud	□		
K Migration Factory (Court Waves)	Azure Government	□		
K Migration Factory (Court Waves)	Google Cloud for Government	□		
K Migration Factory (Court Waves)	Oracle NSR	□		
L Training, Readiness & Change Management	AWS GovCloud	□		
L Training, Readiness & Change Management	Azure Government	□		
L Training, Readiness & Change Management	Google Cloud for Government	□		
L Training, Readiness & Change Management	Oracle NSR	□		

Court Executive Signature: _____ Date: _____

Migration Lead Signature: _____ Date: _____

G.3 Wave 4 — Court Sign-off Sheet

Domain	Cloud	Checklist Complete (□/☑)	Evidence Link	Approver (Name/Date)
A Landing Zones & Guardrails	AWS GovCloud	□		
A Landing Zones & Guardrails	Azure Government	□		
A Landing Zones & Guardrails	Google Cloud for Government	□		
A Landing Zones & Guardrails	Oracle NSR	□		
B Identity & Access	AWS GovCloud	□		
B Identity & Access	Azure Government	□		
B Identity & Access	Google Cloud for Government	□		
B Identity & Access	Oracle NSR	□		
C Networking & Connectivity	AWS GovCloud	□		
C Networking & Connectivity	Azure Government	□		
C Networking & Connectivity	Google Cloud for Government	□		

C Networking & Connectivity	Oracle NSR	☐		
D Security, RMF/ATO	AWS GovCloud	☐		
D Security, RMF/ATO	Azure Government	☐		
D Security, RMF/ATO	Google Cloud for Government	☐		
D Security, RMF/ATO	Oracle NSR	☐		
E Logging, Monitoring & Observability	AWS GovCloud	☐		
E Logging, Monitoring & Observability	Azure Government	☐		
E Logging, Monitoring & Observability	Google Cloud for Government	☐		
E Logging, Monitoring & Observability	Oracle NSR	☐		
F Data Platform (Lakehouse)	AWS GovCloud	☐		
F Data Platform (Lakehouse)	Azure Government	☐		
F Data Platform (Lakehouse)	Google Cloud for Government	☐		
F Data Platform (Lakehouse)	Oracle NSR	☐		
G Application Platforms (Kubernetes/Serverless)	AWS GovCloud	☐		
G Application Platforms (Kubernetes/Serverless)	Azure Government	☐		
G Application Platforms (Kubernetes/Serverless)	Google Cloud for Government	☐		
G Application Platforms (Kubernetes/Serverless)	Oracle NSR	☐		
H DevSecOps & Software Supply Chain	AWS GovCloud	☐		
H DevSecOps & Software Supply Chain	Azure Government	☐		
H DevSecOps & Software Supply Chain	Google Cloud for Government	☐		
H DevSecOps & Software Supply Chain	Oracle NSR	☐		
I Operations: ITSM + SRE + DR/BCP	AWS GovCloud	☐		
I Operations: ITSM + SRE + DR/BCP	Azure Government	☐		
I Operations: ITSM + SRE + DR/BCP	Google Cloud for Government	☐		

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Page 71 of 117

I Operations: ITSM + SRE + DR/BCP	Oracle NSR	☐		
J FinOps & Cost Governance	AWS GovCloud	☐		
J FinOps & Cost Governance	Azure Government	☐		
J FinOps & Cost Governance	Google Cloud for Government	☐		
J FinOps & Cost Governance	Oracle NSR	☐		
K Migration Factory (Court Waves)	AWS GovCloud	☐		
K Migration Factory (Court Waves)	Azure Government	☐		
K Migration Factory (Court Waves)	Google Cloud for Government	☐		
K Migration Factory (Court Waves)	Oracle NSR	☐		
L Training, Readiness & Change Management	AWS GovCloud	☐		
L Training, Readiness & Change Management	Azure Government	☐		
L Training, Readiness & Change Management	Google Cloud for Government	☐		
L Training, Readiness & Change Management	Oracle NSR	☐		

Court Executive Signature: _____ Date: _____

Migration Lead Signature: _____ Date: _____

G.3 Wave 5 — Court Sign-off Sheet

Domain	Cloud	Checklist Complete (☐/☑)	Evidence Link	Approver (Name/Date)
A Landing Zones & Guardrails	AWS GovCloud	☐		
A Landing Zones & Guardrails	Azure Government	☐		
A Landing Zones & Guardrails	Google Cloud for Government	☐		
A Landing Zones & Guardrails	Oracle NSR	☐		
B Identity & Access	AWS GovCloud	☐		
B Identity & Access	Azure Government	☐		
B Identity & Access	Google Cloud for Government	☐		

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

B Identity & Access	Oracle NSR	☐		
C Networking & Connectivity	AWS GovCloud	☐		
C Networking & Connectivity	Azure Government	☐		
C Networking & Connectivity	Google Cloud for Government	☐		
C Networking & Connectivity	Oracle NSR	☐		
D Security, RMF/ATO	AWS GovCloud	☐		
D Security, RMF/ATO	Azure Government	☐		
D Security, RMF/ATO	Google Cloud for Government	☐		
D Security, RMF/ATO	Oracle NSR	☐		
E Logging, Monitoring & Observability	AWS GovCloud	☐		
E Logging, Monitoring & Observability	Azure Government	☐		
E Logging, Monitoring & Observability	Google Cloud for Government	☐		
E Logging, Monitoring & Observability	Oracle NSR	☐		
F Data Platform (Lakehouse)	AWS GovCloud	☐		
F Data Platform (Lakehouse)	Azure Government	☐		
F Data Platform (Lakehouse)	Google Cloud for Government	☐		
F Data Platform (Lakehouse)	Oracle NSR	☐		
G Application Platforms (Kubernetes/Serverless)	AWS GovCloud	☐		
G Application Platforms (Kubernetes/Serverless)	Azure Government	☐		
G Application Platforms (Kubernetes/Serverless)	Google Cloud for Government	☐		
G Application Platforms (Kubernetes/Serverless)	Oracle NSR	☐		
H DevSecOps & Software Supply Chain	AWS GovCloud	☐		
H DevSecOps & Software Supply Chain	Azure Government	☐		
H DevSecOps & Software Supply Chain	Google Cloud for Government	☐		
H DevSecOps & Software Supply Chain	Oracle NSR	☐		

Domain	Cloud	Checklist Complete (□/☑)	Evidence Link	Approver (Name/Date)
I Operations: ITSM + SRE + DR/BCP	AWS GovCloud	□		
I Operations: ITSM + SRE + DR/BCP	Azure Government	□		
I Operations: ITSM + SRE + DR/BCP	Google Cloud for Government	□		
I Operations: ITSM + SRE + DR/BCP	Oracle NSR	□		
J FinOps & Cost Governance	AWS GovCloud	□		
J FinOps & Cost Governance	Azure Government	□		
J FinOps & Cost Governance	Google Cloud for Government	□		
J FinOps & Cost Governance	Oracle NSR	□		
K Migration Factory (Court Waves)	AWS GovCloud	□		
K Migration Factory (Court Waves)	Azure Government	□		
K Migration Factory (Court Waves)	Google Cloud for Government	□		
K Migration Factory (Court Waves)	Oracle NSR	□		
L Training, Readiness & Change Management	AWS GovCloud	□		
L Training, Readiness & Change Management	Azure Government	□		
L Training, Readiness & Change Management	Google Cloud for Government	□		
L Training, Readiness & Change Management	Oracle NSR	□		

Court Executive Signature: _____ Date: _____

Migration Lead Signature: _____ Date: _____

G.3 Wave 6 — Court Sign-off Sheet

Domain	Cloud	Checklist Complete (□/☑)	Evidence Link	Approver (Name/Date)
A Landing Zones & Guardrails	AWS GovCloud	□		
A Landing Zones & Guardrails	Azure Government	□		
A Landing Zones & Guardrails	Google Cloud for Government	□		

A Landing Zones & Guardrails	Oracle NSR	☐		
B Identity & Access	AWS GovCloud	☐		
B Identity & Access	Azure Government	☐		
B Identity & Access	Google Cloud for Government	☐		
B Identity & Access	Oracle NSR	☐		
C Networking & Connectivity	AWS GovCloud	☐		
C Networking & Connectivity	Azure Government	☐		
C Networking & Connectivity	Google Cloud for Government	☐		
C Networking & Connectivity	Oracle NSR	☐		
D Security, RMF/ATO	AWS GovCloud	☐		
D Security, RMF/ATO	Azure Government	☐		
D Security, RMF/ATO	Google Cloud for Government	☐		
D Security, RMF/ATO	Oracle NSR	☐		
E Logging, Monitoring & Observability	AWS GovCloud	☐		
E Logging, Monitoring & Observability	Azure Government	☐		
E Logging, Monitoring & Observability	Google Cloud for Government	☐		
E Logging, Monitoring & Observability	Oracle NSR	☐		
F Data Platform (Lakehouse)	AWS GovCloud	☐		
F Data Platform (Lakehouse)	Azure Government	☐		
F Data Platform (Lakehouse)	Google Cloud for Government	☐		
F Data Platform (Lakehouse)	Oracle NSR	☐		
G Application Platforms (Kubernetes/Serverless)	AWS GovCloud	☐		
G Application Platforms (Kubernetes/Serverless)	Azure Government	☐		
G Application Platforms (Kubernetes/Serverless)	Google Cloud for Government	☐		
G Application Platforms (Kubernetes/Serverless)	Oracle NSR	☐		

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

H DevSecOps & Software Supply Chain	AWS GovCloud	☐		
H DevSecOps & Software Supply Chain	Azure Government	☐		
H DevSecOps & Software Supply Chain	Google Cloud for Government	☐		
H DevSecOps & Software Supply Chain	Oracle NSR	☐		
I Operations: ITSM + SRE + DR/BCP	AWS GovCloud	☐		
I Operations: ITSM + SRE + DR/BCP	Azure Government	☐		
I Operations: ITSM + SRE + DR/BCP	Google Cloud for Government	☐		
I Operations: ITSM + SRE + DR/BCP	Oracle NSR	☐		
J FinOps & Cost Governance	AWS GovCloud	☐		
J FinOps & Cost Governance	Azure Government	☐		
J FinOps & Cost Governance	Google Cloud for Government	☐		
J FinOps & Cost Governance	Oracle NSR	☐		
K Migration Factory (Court Waves)	AWS GovCloud	☐		
K Migration Factory (Court Waves)	Azure Government	☐		
K Migration Factory (Court Waves)	Google Cloud for Government	☐		
K Migration Factory (Court Waves)	Oracle NSR	☐		
L Training, Readiness & Change Management	AWS GovCloud	☐		
L Training, Readiness & Change Management	Azure Government	☐		
L Training, Readiness & Change Management	Google Cloud for Government	☐		
L Training, Readiness & Change Management	Oracle NSR	☐		

Court Executive Signature: _____ Date: _____

Migration Lead Signature: _____ Date: _____

G.3 Wave 7 — Court Sign-off Sheet

Domain	Cloud	Checklist Complete (□/☑)	Evidence Link	Approver (Name/Date)
A Landing Zones & Guardrails	AWS GovCloud	□		
A Landing Zones & Guardrails	Azure Government	□		
A Landing Zones & Guardrails	Google Cloud for Government	□		
A Landing Zones & Guardrails	Oracle NSR	□		
B Identity & Access	AWS GovCloud	□		
B Identity & Access	Azure Government	□		
B Identity & Access	Google Cloud for Government	□		
B Identity & Access	Oracle NSR	□		
C Networking & Connectivity	AWS GovCloud	□		
C Networking & Connectivity	Azure Government	□		
C Networking & Connectivity	Google Cloud for Government	□		
C Networking & Connectivity	Oracle NSR	□		
D Security, RMF/ATO	AWS GovCloud	□		
D Security, RMF/ATO	Azure Government	□		
D Security, RMF/ATO	Google Cloud for Government	□		
D Security, RMF/ATO	Oracle NSR	□		
E Logging, Monitoring & Observability	AWS GovCloud	□		
E Logging, Monitoring & Observability	Azure Government	□		
E Logging, Monitoring & Observability	Google Cloud for Government	□		
E Logging, Monitoring & Observability	Oracle NSR	□		
F Data Platform (Lakehouse)	AWS GovCloud	□		
F Data Platform (Lakehouse)	Azure Government	□		
F Data Platform (Lakehouse)	Google Cloud for Government	□		

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

F Data Platform (Lakehouse)	Oracle NSR	☐		
G Application Platforms (Kubernetes/Serverless)	AWS GovCloud	☐		
G Application Platforms (Kubernetes/Serverless)	Azure Government	☐		
G Application Platforms (Kubernetes/Serverless)	Google Cloud for Government	☐		
G Application Platforms (Kubernetes/Serverless)	Oracle NSR	☐		
H DevSecOps & Software Supply Chain	AWS GovCloud	☐		
H DevSecOps & Software Supply Chain	Azure Government	☐		
H DevSecOps & Software Supply Chain	Google Cloud for Government	☐		
H DevSecOps & Software Supply Chain	Oracle NSR	☐		
I Operations: ITSM + SRE + DR/BCP	AWS GovCloud	☐		
I Operations: ITSM + SRE + DR/BCP	Azure Government	☐		
I Operations: ITSM + SRE + DR/BCP	Google Cloud for Government	☐		
I Operations: ITSM + SRE + DR/BCP	Oracle NSR	☐		
J FinOps & Cost Governance	AWS GovCloud	☐		
J FinOps & Cost Governance	Azure Government	☐		
J FinOps & Cost Governance	Google Cloud for Government	☐		
J FinOps & Cost Governance	Oracle NSR	☐		
K Migration Factory (Court Waves)	AWS GovCloud	☐		
K Migration Factory (Court Waves)	Azure Government	☐		
K Migration Factory (Court Waves)	Google Cloud for Government	☐		
K Migration Factory (Court Waves)	Oracle NSR	☐		
L Training, Readiness & Change Management	AWS GovCloud	☐		
L Training, Readiness & Change Management	Azure Government	☐		

Domain	Cloud	Checklist Complete (☐/☑)		
L Training, Readiness & Change Management	Google Cloud for Government	☐		
L Training, Readiness & Change Management	Oracle NSR	☐		

Court Executive Signature: _____ Date: _____

Migration Lead Signature: _____ Date: _____

G.3 Wave 8 — Court Sign-off Sheet

Domain	Cloud	Checklist Complete (☐/☑)	Evidence Link	Approver (Name/Date)
A Landing Zones & Guardrails	AWS GovCloud	☐		
A Landing Zones & Guardrails	Azure Government	☐		
A Landing Zones & Guardrails	Google Cloud for Government	☐		
A Landing Zones & Guardrails	Oracle NSR	☐		
B Identity & Access	AWS GovCloud	☐		
B Identity & Access	Azure Government	☐		
B Identity & Access	Google Cloud for Government	☐		
B Identity & Access	Oracle NSR	☐		
C Networking & Connectivity	AWS GovCloud	☐		
C Networking & Connectivity	Azure Government	☐		
C Networking & Connectivity	Google Cloud for Government	☐		
C Networking & Connectivity	Oracle NSR	☐		
D Security, RMF/ATO	AWS GovCloud	☐		
D Security, RMF/ATO	Azure Government	☐		
D Security, RMF/ATO	Google Cloud for Government	☐		
D Security, RMF/ATO	Oracle NSR	☐		
E Logging, Monitoring & Observability	AWS GovCloud	☐		
E Logging, Monitoring & Observability	Azure Government	☐		
E Logging, Monitoring & Observability	Google Cloud for Government	☐		

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

E Logging, Monitoring & Observability	Oracle NSR	☐		
F Data Platform (Lakehouse)	AWS GovCloud	☐		
F Data Platform (Lakehouse)	Azure Government	☐		
F Data Platform (Lakehouse)	Google Cloud for Government	☐		
F Data Platform (Lakehouse)	Oracle NSR	☐		
G Application Platforms (Kubernetes/Serverless)	AWS GovCloud	☐		
G Application Platforms (Kubernetes/Serverless)	Azure Government	☐		
G Application Platforms (Kubernetes/Serverless)	Google Cloud for Government	☐		
G Application Platforms (Kubernetes/Serverless)	Oracle NSR	☐		
H DevSecOps & Software Supply Chain	AWS GovCloud	☐		
H DevSecOps & Software Supply Chain	Azure Government	☐		
H DevSecOps & Software Supply Chain	Google Cloud for Government	☐		
H DevSecOps & Software Supply Chain	Oracle NSR	☐		
I Operations: ITSM + SRE + DR/BCP	AWS GovCloud	☐		
I Operations: ITSM + SRE + DR/BCP	Azure Government	☐		
I Operations: ITSM + SRE + DR/BCP	Google Cloud for Government	☐		
I Operations: ITSM + SRE + DR/BCP	Oracle NSR	☐		
J FinOps & Cost Governance	AWS GovCloud	☐		
J FinOps & Cost Governance	Azure Government	☐		
J FinOps & Cost Governance	Google Cloud for Government	☐		
J FinOps & Cost Governance	Oracle NSR	☐		
K Migration Factory (Court Waves)	AWS GovCloud	☐		
K Migration Factory (Court Waves)	Azure Government	☐		

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Domain	Cloud	Checklist Complete (□/☑)	Evidence Link	Approver (Name/Date)
K Migration Factory (Court Waves)	Google Cloud for Government	□		
K Migration Factory (Court Waves)	Oracle NSR	□		
L Training, Readiness & Change Management	AWS GovCloud	□		
L Training, Readiness & Change Management	Azure Government	□		
L Training, Readiness & Change Management	Google Cloud for Government	□		
L Training, Readiness & Change Management	Oracle NSR	□		

Court Executive Signature: _____ Date: _____

Migration Lead Signature: _____ Date: _____

G.3 Wave 9 — Court Sign-off Sheet

Domain	Cloud	Checklist Complete (□/☑)	Evidence Link	Approver (Name/Date)
A Landing Zones & Guardrails	AWS GovCloud	□		
A Landing Zones & Guardrails	Azure Government	□		
A Landing Zones & Guardrails	Google Cloud for Government	□		
A Landing Zones & Guardrails	Oracle NSR	□		
B Identity & Access	AWS GovCloud	□		
B Identity & Access	Azure Government	□		
B Identity & Access	Google Cloud for Government	□		
B Identity & Access	Oracle NSR	□		
C Networking & Connectivity	AWS GovCloud	□		
C Networking & Connectivity	Azure Government	□		
C Networking & Connectivity	Google Cloud for Government	□		
C Networking & Connectivity	Oracle NSR	□		
D Security, RMF/ATO	AWS GovCloud	□		
D Security, RMF/ATO	Azure Government	□		
D Security, RMF/ATO	Google Cloud for Government	□		

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

D Security, RMF/ATO	Oracle NSR	☐		
E Logging, Monitoring & Observability	AWS GovCloud	☐		
E Logging, Monitoring & Observability	Azure Government	☐		
E Logging, Monitoring & Observability	Google Cloud for Government	☐		
E Logging, Monitoring & Observability	Oracle NSR	☐		
F Data Platform (Lakehouse)	AWS GovCloud	☐		
F Data Platform (Lakehouse)	Azure Government	☐		
F Data Platform (Lakehouse)	Google Cloud for Government	☐		
F Data Platform (Lakehouse)	Oracle NSR	☐		
G Application Platforms (Kubernetes/Serverless)	AWS GovCloud	☐		
G Application Platforms (Kubernetes/Serverless)	Azure Government	☐		
G Application Platforms (Kubernetes/Serverless)	Google Cloud for Government	☐		
G Application Platforms (Kubernetes/Serverless)	Oracle NSR	☐		
H DevSecOps & Software Supply Chain	AWS GovCloud	☐		
H DevSecOps & Software Supply Chain	Azure Government	☐		
H DevSecOps & Software Supply Chain	Google Cloud for Government	☐		
H DevSecOps & Software Supply Chain	Oracle NSR	☐		
I Operations: ITSM + SRE + DR/BCP	AWS GovCloud	☐		
I Operations: ITSM + SRE + DR/BCP	Azure Government	☐		
I Operations: ITSM + SRE + DR/BCP	Google Cloud for Government	☐		
I Operations: ITSM + SRE + DR/BCP	Oracle NSR	☐		
J FinOps & Cost Governance	AWS GovCloud	☐		
J FinOps & Cost Governance	Azure Government	☐		
J FinOps & Cost Governance	Google Cloud for Government	☐		

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Domain	Cloud	Checklist Complete (☐/☑)	Evidence Link	Approver (Name/Date)
J FinOps & Cost Governance	Oracle NSR	☐		
K Migration Factory (Court Waves)	AWS GovCloud	☐		
K Migration Factory (Court Waves)	Azure Government	☐		
K Migration Factory (Court Waves)	Google Cloud for Government	☐		
K Migration Factory (Court Waves)	Oracle NSR	☐		
L Training, Readiness & Change Management	AWS GovCloud	☐		
L Training, Readiness & Change Management	Azure Government	☐		
L Training, Readiness & Change Management	Google Cloud for Government	☐		
L Training, Readiness & Change Management	Oracle NSR	☐		

Court Executive Signature: _____ Date: _____

Migration Lead Signature: _____ Date: _____

G.3 Wave 10 — Court Sign-off Sheet

Domain	Cloud	Checklist Complete (☐/☑)	Evidence Link	Approver (Name/Date)
A Landing Zones & Guardrails	AWS GovCloud	☐		
A Landing Zones & Guardrails	Azure Government	☐		
A Landing Zones & Guardrails	Google Cloud for Government	☐		
A Landing Zones & Guardrails	Oracle NSR	☐		
B Identity & Access	AWS GovCloud	☐		
B Identity & Access	Azure Government	☐		
B Identity & Access	Google Cloud for Government	☐		
B Identity & Access	Oracle NSR	☐		
C Networking & Connectivity	AWS GovCloud	☐		
C Networking & Connectivity	Azure Government	☐		
C Networking & Connectivity	Google Cloud for Government	☐		

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

C Networking & Connectivity	Oracle NSR	☐		
D Security, RMF/ATO	AWS GovCloud	☐		
D Security, RMF/ATO	Azure Government	☐		
D Security, RMF/ATO	Google Cloud for Government	☐		
D Security, RMF/ATO	Oracle NSR	☐		
E Logging, Monitoring & Observability	AWS GovCloud	☐		
E Logging, Monitoring & Observability	Azure Government	☐		
E Logging, Monitoring & Observability	Google Cloud for Government	☐		
E Logging, Monitoring & Observability	Oracle NSR	☐		
F Data Platform (Lakehouse)	AWS GovCloud	☐		
F Data Platform (Lakehouse)	Azure Government	☐		
F Data Platform (Lakehouse)	Google Cloud for Government	☐		
F Data Platform (Lakehouse)	Oracle NSR	☐		
G Application Platforms (Kubernetes/Serverless)	AWS GovCloud	☐		
G Application Platforms (Kubernetes/Serverless)	Azure Government	☐		
G Application Platforms (Kubernetes/Serverless)	Google Cloud for Government	☐		
G Application Platforms (Kubernetes/Serverless)	Oracle NSR	☐		
H DevSecOps & Software Supply Chain	AWS GovCloud	☐		
H DevSecOps & Software Supply Chain	Azure Government	☐		
H DevSecOps & Software Supply Chain	Google Cloud for Government	☐		
H DevSecOps & Software Supply Chain	Oracle NSR	☐		
I Operations: ITSM + SRE + DR/BCP	AWS GovCloud	☐		
I Operations: ITSM + SRE + DR/BCP	Azure Government	☐		
I Operations: ITSM + SRE + DR/BCP	Google Cloud for Government	☐		

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Page 84 of 117

I Operations: ITSM + SRE + DR/BCP	Oracle NSR	☐			
J FinOps & Cost Governance	AWS GovCloud	☐			
J FinOps & Cost Governance	Azure Government	☐			
J FinOps & Cost Governance	Google Cloud for Government	☐			
J FinOps & Cost Governance	Oracle NSR	☐			
K Migration Factory (Court Waves)	AWS GovCloud	☐			
K Migration Factory (Court Waves)	Azure Government	☐			
K Migration Factory (Court Waves)	Google Cloud for Government	☐			
K Migration Factory (Court Waves)	Oracle NSR	☐			
L Training, Readiness & Change Management	AWS GovCloud	☐			
L Training, Readiness & Change Management	Azure Government	☐			
L Training, Readiness & Change Management	Google Cloud for Government	☐			
L Training, Readiness & Change Management	Oracle NSR	☐			

Court Executive Signature: _____ Date: _____

Migration Lead Signature: _____ Date: _____

Appendix H — KPI Definition Catalog

KPI	Definition / Calculation	Target	Data Source	Owner	Refresh Cadence
Policy Compliance	(# green policies ÷ total)	≥98%	Config/Policy scanners	CCoE Security	Weekly
Private PaaS Coverage	(# services on private ÷ critical services)	100%	Cloud inventories	Network	Monthly
DQ Pass Rate	(# checks passed ÷ checks run)	≥99%	DQ engine	Data	Daily
Provenance Coverage	(# releases with attestations ÷ total releases)	100%	CI/CD	DevSecOps	Per Release
SLO Attainment	(% of periods within SLO)	≥99%	SRE dashboards	SRE	Weekly
Cost Variance	((Actual-Budget) ÷ Budget)	±5%	FinOps dashboards	FinOps	Monthly

Wave On-Time	(# waves on schedule ÷ total)	≥90%	PMO IMS	PMO	Weekly
DR Test Pass	(# successful tests ÷ total DR tests)	100%	DR reports	Ops	Quarterly
Alert ACK Time	Mean minutes to acknowledge	< 5m	SIEM/On-call	SRE	Weekly
MTTR (P1)	Mean Time To Restore (minutes)	< 30m	Incident tracker	SRE	Weekly
Tag Compliance	(Tagged resources ÷ total)	≥95%	Cloud inventory	FinOps	Monthly

Appendix I — Control Matrix Crosswalk (Excerpt)

NIST 800-53 Rev.5	Implementation (Multi-Cloud)	Evidence	Inherited/Customer
AC-2 Account Management	Federated IdP, SCIM/JIT, quarterly reviews	Access review logs	Customer
AC-4 Info Flow Enforcement	NGFW/L7 policies, segmentation, RPZ	Firewall configs, RPZ exports	Customer
AU-2 Auditable Events	CloudTrail/Activity Logs/Chronicle + SIEM	SIEM rules, retention settings	Shared
CM-6 Config Settings	IaC modules + Policy-as-Code gates	Repo links, pipeline logs	Customer
IA-2 Identification & Auth	CAC/PIV + MFA enforced	IdP policy, auth logs	Shared
IR-4 Incident Handling	IR runbooks, on-call rota, tabletop exercises	AARs, tickets	Customer
RA-5 Vulnerability Scanning	SAST/SCA/DAST/IAST + infra scans	Reports, SARIF bundles	Customer
SC-12/13 Cryptography	KMS/Key Vault/Cloud KMS/Vault; FIPS 140-3	Key policies, rotation logs	Shared
SI-4 Monitoring	Native detections + SIEM correlation	Alert exports	Shared
PL-8 Security Architecture	ZTA patterns; LZ guardrails	Diagrams, ADRs	Customer

Appendix J — Data Classification & Tagging Schema

Tag Key	Description	Examples / Allowed Values	Required (Y/N)
court_id	Unique court or program identifier	e.g., CT-023	Y
env	Environment stage	dev,test,stage,prod	Y
data_class	Sensitivity classification	PII, PHI, CJIS, CUI, public	Y
owner	Business owner	Org/Team	Y
cost_center	Chargeback/showback key	GL/COA code	Y
system	System/application identifier	e.g., docketing, case-mgr	Y

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

dr_tier	DR criticality tier	tier-1, tier-2, tier-3	N
slo	Target SLO bucket	99.9, 99.99	N

Appendix K — RACI Master (CCoE & Domains)

Activity	R	A	C	I
Define & approve scope/objectives	EA Lead	CTO	CCoE, PMO	Court Execs
Stand up LZ MVP	Cloud Platform Leads	CTO	Security, Network	Court IT
Establish governance (ARB/CCB/ECAB)	CCoE Lead	CISO	EA, PMO	All Stakeholders
Publish tagging & data classification	Security	CISO	Data, Courts	Platform
Define acceptance criteria & KPIs	PMO	CTO	All domain leads	Court Execs
Wave readiness gating	Migration Lead	PMO	Courts, Security, Data	CCoE

Appendix L — Milestone Exit Criteria Test Procedures

Milestone	Test Procedure	Pass/Fail	Evidence	Owner
M1: LZ MVP	Run conformance packs; verify policy ≥90%; private access tested			
M3: Private PaaS	Validate endpoints (PE/PL/PSC/SG); ensure no public egress			
M6: Data & DevSecOps	DQ ≥99%; provenance required to deploy; dashboards live			
M9: App Platform GA	Blue/green + canary drills; pod MTTR < 5m			
M12: 50 Courts	Zero P1 at go-live; reconciliation 100%			
M18: 300 Courts	All waves complete; optimization backlog operating			

Appendix M — CDRL Traceability Matrix

CDRL/Deliverable	Proposal Section(s)	Acceptance Criteria (summary)
PMP / IMS	2 Governance; 17 Roadmap	Approved plan + milestones; baselines tracked
RAID Log	18 Risks and RAID Log	Updated weekly; owners assigned
Security Strategy / RMF Plan	7 Security; 8 Logging; Appendix SOC	Assessor dry-run green; dashboards live
LZ Designs (per cloud)	4 Landing Zones	Conformance/drift tests pass; PAW/JIT validated
Data Platform Design	9 Data Platform	DQ ≥99%; lineage present; SLAs signed
DevSecOps Playbooks	11 DevSecOps	SLSA/provenance enforced; 0 critical vulns at release
Training Plan	16 Training	≥95% completion; ≥80% proficiency
Migration Plan (Court Waves)	15 Migration Factory	Go-live with 0 P1; reconciliation 100%

Appendix N — Base Kit Inventory (Excerpt)

File Path
CCoE_Build_Kit_v1_300Courts/
CCoE_Build_Kit_v1_300Courts/00_START/
CCoE_Build_Kit_v1_300Courts/00_START/00_Cover_Sheet.docx
CCoE_Build_Kit_v1_300Courts/00_START/01_Executive_Overview.docx
CCoE_Build_Kit_v1_300Courts/00_START/02_Terminology_and_Acronyms.docx
CCoE_Build_Kit_v1_300Courts/00_START/03_Objectives_and_Scope.docx
CCoE_Build_Kit_v1_300Courts/00_START/04_Stakeholders_and_Roles.docx
CCoE_Build_Kit_v1_300Courts/00_START/05_Security_Markings_and_Submission_Conventions.docx
CCoE_Build_Kit_v1_300Courts/00_START/06_Program_Governance_Overview.docx
CCoE_Build_Kit_v1_300Courts/00_START/07_Discovery_and_Inventory_Method.docx
CCoE_Build_Kit_v1_300Courts/00_START/08_Data_Classification_and_Tagging_Baseline.docx
CCoE_Build_Kit_v1_300Courts/00_START/09_Security_Roles_per_Court_and_Access_Control.docx
CCoE_Build_Kit_v1_300Courts/00_START/10_Identity_and_Network_Baseline_Ingress_Egress.docx
CCoE_Build_Kit_v1_300Courts/00_START/11_Cloud_Selection_Framework.docx
CCoE_Build_Kit_v1_300Courts/00_START/12_CICD_and_Software_Factory_Baseline.docx
CCoE_Build_Kit_v1_300Courts/00_START/13_AI_ML_Governance_Basics.docx
CCoE_Build_Kit_v1_300Courts/00_START/14_ATO_Overview_and_Artifact_Map.docx
CCoE_Build_Kit_v1_300Courts/00_START/15_Onboarding_Checklist_Per_Court.docx
CCoE_Build_Kit_v1_300Courts/00_START/16_Document_Control_and_Change_Log.docx
CCoE_Build_Kit_v1_300Courts/00_START/17_00_START_Index_of_Documents.docx
CCoE_Build_Kit_v1_300Courts/10_STRATEGY/
CCoE_Build_Kit_v1_300Courts/10_STRATEGY/00_Cover_Sheet.docx
CCoE_Build_Kit_v1_300Courts/10_STRATEGY/01_Terminology_and_Acronyms.docx
CCoE_Build_Kit_v1_300Courts/10_STRATEGY/02_Contract_Baseline_and_Interpretations.docx
CCoE_Build_Kit_v1_300Courts/10_STRATEGY/03_Deliverables_Matrix_(CDRL)_and_Acceptance_Criteria.docx
CCoE_Build_Kit_v1_300Courts/10_STRATEGY/04_Program_Management_Plan_(PMP).docx
CCoE_Build_Kit_v1_300Courts/10_STRATEGY/05_Integrated_Master_Schedule_(IMS)_and_Milestones.docx
CCoE_Build_Kit_v1_300Courts/10_STRATEGY/06_Transition-In_Plan_(0-30-60-90).docx
CCoE_Build_Kit_v1_300Courts/10_STRATEGY/07_Operating_Cadence_and_Calendar.docx
CCoE_Build_Kit_v1_300Courts/10_STRATEGY/08_Risk-Issue-Decision_(RAID)_Log_Strategy.docx
CCoE_Build_Kit_v1_300Courts/10_STRATEGY/09_Stakeholder_Engagement_&_Comms_Plan.docx
CCoE_Build_Kit_v1_300Courts/10_STRATEGY/10_Court_Segmentation_&_Wave_Strategy.docx
CCoE_Build_Kit_v1_300Courts/10_STRATEGY/11_Provider_Selection_Application.docx
CCoE_Build_Kit_v1_300Courts/10_STRATEGY/12_Migration_Strategy_&_Readiness_Gates.docx
CCoE_Build_Kit_v1_300Courts/10_STRATEGY/13_Quality_Assurance_&_Test_Strategy.docx
CCoE_Build_Kit_v1_300Courts/10_STRATEGY/14_Change_Management_(Org_Change_&_Training).docx
CCoE_Build_Kit_v1_300Courts/10_STRATEGY/15_Security_Privacy_&_ATO_Execution_Strategy.docx
CCoE_Build_Kit_v1_300Courts/10_STRATEGY/16_Data_Governance_Retention_eDiscovery_Legal_Holds.docx
CCoE_Build_Kit_v1_300Courts/10_STRATEGY/17_FinOps_&_Budget_Management_Strategy.docx
CCoE_Build_Kit_v1_300Courts/10_STRATEGY/18_Reporting_&_Dashboards.docx
CCoE_Build_Kit_v1_300Courts/10_STRATEGY/19_Exit_&_Transition-Out_Strategy.docx
CCoE_Build_Kit_v1_300Courts/10_STRATEGY/20_Index_of_Documents.docx
CCoE_Build_Kit_v1_300Courts/20_GOVERNANCE/

CCoE_Build_Kit_v1_300Courts/20_GOVERNANCE/00_Cover_Sheet.docx
CCoE_Build_Kit_v1_300Courts/20_GOVERNANCE/01_Terminology_and_Acronyms.docx
CCoE_Build_Kit_v1_300Courts/20_GOVERNANCE/02_CCOE_Charter.docx
CCoE_Build_Kit_v1_300Courts/20_GOVERNANCE/02_RACI.csv
CCoE_Build_Kit_v1_300Courts/20_GOVERNANCE/03_Delegation_of_Authority.docx
CCoE_Build_Kit_v1_300Courts/20_GOVERNANCE/04_RACI.docx
CCoE_Build_Kit_v1_300Courts/20_GOVERNANCE/05_Governance_Model.docx
CCoE_Build_Kit_v1_300Courts/20_GOVERNANCE/06_ARB_Charter.docx
CCoE_Build_Kit_v1_300Courts/20_GOVERNANCE/07_CCB_Charter.docx
CCoE_Build_Kit_v1_300Courts/20_GOVERNANCE/08_Policy_as_Code_Standard.docx
CCoE_Build_Kit_v1_300Courts/20_GOVERNANCE/09_Exceptions_Workflow.docx
CCoE_Build_Kit_v1_300Courts/20_GOVERNANCE/10_Change_Types_and_Workflow.docx
CCoE_Build_Kit_v1_300Courts/20_GOVERNANCE/11_Metrics_OKRs_and_Dashboards.docx
CCoE_Build_Kit_v1_300Courts/20_GOVERNANCE/12_Audit_and_Reporting_Schedule.docx
CCoE_Build_Kit_v1_300Courts/20_GOVERNANCE/13_Compliance_Mapping.docx
CCoE_Build_Kit_v1_300Courts/20_GOVERNANCE/14_Governance_Communications_Plan.docx
CCoE_Build_Kit_v1_300Courts/20_GOVERNANCE/15_Decision_Log_Template.docx
CCoE_Build_Kit_v1_300Courts/20_GOVERNANCE/16_Governance_Onboarding_For_Court.docx
CCoE_Build_Kit_v1_300Courts/20_GOVERNANCE/17_Index_of_Documents.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/00_Cover_Sheet.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/01_Terminology_and_Acronyms.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/02_Architecture_Methodology_and_Principles.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/03_Provider_Selection_Decision_Matrix.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/04_Scenario_Decision_Trees.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/05_Service_Equivalency_Matrix_AWS_Azure_GCP_OCI.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/06_MultiCloud_and_Sovereignty_Patterns.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/07_Network_Connectivity_Patterns.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/08_Security_and_Controls_Map_Common.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/09_Data_Classification_and_Encryption_Architecture.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/10_VMWare_to_Cloud_Strategies.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/11_Containers_and_Serverless_Platforms.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/12_Patterns_Catalog_Index.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/13_Shared_Responsibility_Overlays_by_Layer.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/14_Service_Inventory_by_Layer.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/20_AWS_Data_Platform_and_Analytics.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/20_AWS_Deployment_IaC_Standards.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/20_AWS_IaaS_Standards_and_Baselines.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/20_AWS_Identity_and_Access.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/20_AWS_Landing_Zone_Design.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/20_AWS_Logging_Monitoring_SIEM.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/20_AWS_Network_Ingress_Egress.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/20_AWS_PaaS_Patterns_and_Guardrails.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/20_AWS_PaaS_Service_Catalog.docx

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/20_AWS_Reference_Architecture.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/20_AWS_Resilience_and_DR.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/20_AWS_SaaS_Integration_and_Governance.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/20_AWS_Security_Controls_Map.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/30_Azure_Data_Platform_and_Analytics.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/30_Azure_Deployment_IaC_Standards.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/30_Azure_IaaS_Standards_and_Baselines.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/30_Azure_Identity_and_Access.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/30_Azure_Landing_Zone_Design.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/30_Azure_Logging_Monitoring_SIEM.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/30_Azure_Network_Ingress_Egress.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/30_Azure_PaaS_Patterns_and_Guardrails.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/30_Azure_PaaS_Service_Catalog.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/30_Azure_Reference_Architecture.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/30_Azure_Resilience_and_DR.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/30_Azure_SaaS_Integration_and_Governance.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/30_Azure_Security_Controls_Map.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/40_GCP_Data_Platform_and_Analytics.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/40_GCP_Deployment_IaC_Standards.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/40_GCP_IaaS_Standards_and_Baselines.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/40_GCP_Identity_and_Access.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/40_GCP_Landing_Zone_Design.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/40_GCP_Logging_Monitoring_SIEM.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/40_GCP_Network_Ingress_Egress.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/40_GCP_PaaS_Patterns_and_Guardrails.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/40_GCP_PaaS_Service_Catalog.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/40_GCP_Reference_Architecture.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/40_GCP_Resilience_and_DR.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/40_GCP_SaaS_Integration_and_Governance.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/40_GCP_Security_Controls_Map.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/50_OCI_Data_Platform_and_Analytics.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/50_OCI_Deployment_IaC_Standards.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/50_OCI_IaaS_Standards_and_Baselines.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/50_OCI_Identity_and_Access.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/50_OCI_Landing_Zone_Design.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/50_OCI_Logging_Monitoring_SIEM.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/50_OCI_Network_Ingress_Egress.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/50_OCI_PaaS_Patterns_and_Guardrails.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/50_OCI_PaaS_Service_Catalog.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/50_OCI_Reference_Architecture.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/50_OCI_Resilience_and_DR.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/50_OCI_SaaS_Integration_and_Governance.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/50_OCI_Security_Controls_Map.docx
CCoE_Build_Kit_v1_300Courts/30_ARCHITECTURE/99_Index_of_Documents.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/00_Cover_Sheet.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/01_Terminology_and_Acronyms.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/02_Security_Model_&_Tenancy_Isolation_Overview.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/02_Security_Strategy_Zero_Trust.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/03_Account___Subscription___Project___Compartment_Hierarchies_(All_Clouds).docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/03_Control_Baseline_NIST_800-53_R5.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/04_Data_Protection_and_Encryption.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/04_Identity_&_Access_Architecture.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/05_Identity_and_Privileged_Access_Security.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/05_Privileged_Access_Management_(PAM)_and_Break-Glass.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/06_Logging_SIEM_and_Security_Analytics.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/06_Network_Security_Baselines_—_Ingress___Egress___Segmentation.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/07_Crypto_&_Key_Management_Standard.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/07_Vulnerability_and_Patch_Management.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/08_Data_Tagging_&_Classification_Standard.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/08_Incident_Response_Playbooks_Index.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/09_Continuity_Disaster_Recovery_BCP.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/09_STIG_&_CIS_Hardening_Baselines.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/10_Continuous_Monitoring_Plan.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/10_Vulnerability_&_Patch_Management.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/11_Logging,_Monitoring,_SIEM_&_SOAR_—_CCoE_SOC.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/11_Privacy_PTA_PIA_Framework.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/12_Access_Reviews_and_Certifications.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/12_Detection_Engineering_&_Use_Cases.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/13_Incident_Response_Plan_&_Playbooks.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/13_Key_Management_and_HSM_Operations.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/14_Continuous_Monitoring_(ConMon)_&_ATO_Alignment.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/14_Endpoint_Security_and_Baseline_Hardening.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/15_Control_Mapping_—_NIST_SP_800-53_Rev._5.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/15_Third_Party_Risk_and_Supply_Chain_Security.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/16_Privacy_&_CJIS_Considerations.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/16_Security_Exception_and_Risk_Acceptance.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/17_DLP,_eDiscovery,_and_Legal_Holds.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/17_Index_of_Documents.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/18_Secrets_Management_Standard.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/19_Supply_Chain_Security_(SLSA_SBOM).docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/20_Endpoint_Security_&_Device_Trust_(Admin).docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/21_Insider_Threat_&_Anomaly_Management.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/22_Deception_and_Honey_Tokens.docx

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Page 91 of 117

CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/23_Backup_&_Recovery_Security.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/24_DR_BCP_Security_Validation.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/25_Audit_&_Reporting_Cadence.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/26_Exceptions_&_Risk_Acceptance_Workflow.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/50_AWS_AWS_Data_Protection.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/50_AWS_AWS_Guardrails_(SCP_Config).docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/50_AWS_AWS_Identity_Patterns.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/50_AWS_AWS_Logging_&_SIEM.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/50_AWS_AWS_Network_Security.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/50_AWS_AWS_STIG_CIS_Implementation.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/60_Azure_Azure_Data_Protection.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/60_Azure_Azure_Guardrails_(Policy_Blueprints).docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/60_Azure_Azure_Identity_Patterns.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/60_Azure_Azure_Logging_&_SIEM.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/60_Azure_Azure_Network_Security.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/60_Azure_Azure_STIG_CIS_Implementation.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/70_GCP_GCP_Data_Protection.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/70_GCP_GCP_Guardrails_(Org_Policy).docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/70_GCP_GCP_Identity_Patterns.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/70_GCP_GCP_Logging_&_SIEM.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/70_GCP_GCP_Network_Security.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/70_GCP_GCP_STIG_CIS_Implementation.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/80_OCI_OCI_Data_Protection.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/80_OCI_OCI_Guardrails_(Security_Zones).docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/80_OCI_OCI_Identity_Patterns.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/80_OCI_OCI_Logging_&_SIEM.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/80_OCI_OCI_Network_Security.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/80_OCI_OCI_STIG_CIS_Implementation.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/99_Index_of_Documents.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/ANNEX_User_Uploaded/
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/ANNEX_User_Uploaded/01_ZTA.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/ANNEX_User_Uploaded/02_Data_Classification_and_Tags.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/ANNEX_User_Uploaded/03_Security_Roles_per_Court.docx
CCoE_Build_Kit_v1_300Courts/40_SECURITY_PRIVACY/ANNEX_User_Uploaded/04_Privacy_Plan.docx
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/00_Cover_Sheet.docx
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/01_Infrastructure_Discovery.csv
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/01_Terminology_and_Acronyms.docx
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/02_Discovery_Master_Plan.docx
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/02_Software_Inventory.csv
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/03_Court_Catalog_and_ID_Scheme.docx
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/03_Move_Refactor_Retain.csv
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/04_Roles_and_Staffing_for_Discovery.docx

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Page 92 of 117

CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/04_User_and_Role_Hierarchy.csv
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/05_Data_Flows.csv
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/05_Schedule_and_Waves.docx
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/06_Evidence_Handling_and_Naming_Standards.docx
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/07_Tooling_and_Data_Sources_AWS_Azure_GCP_OCI.docx
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/08_Data_Model_for_CMDB_and_Ingestion.docx
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/09_Deduplication_and_Data_Quality.docx
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/10_Privacy_Security_and_Consent_for_Discovery.docx
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/11_Per-Court_Discovery_Binder_Template_Checklist.docx
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/12_Intake_Form_Court_Overview.docx
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/13_Infrastructure_Inventory_IaaS.docx
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/14_VMware_Discovery.docx
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/15_Network_Discovery.docx
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/16_Application_Portfolio.docx
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/17_Data_Assets_Classification.docx
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/18_SaaS_Licensing.docx
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/19_Identity_Access_Baseline.docx
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/20_Security_Posture_STIG_CIS_Checklist.docx
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/21_Backup_DR_Recovery.docx
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/22_Dependency_Mapping.docx
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/23_Readiness_Scoring_Model.docx
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/24_Cloud_Selection_Questionnaire.docx
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/25_Tagging_Metadata_Standard_Court_Implementation.docx
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/26_Evidence_Capture_Checklist.docx
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/27_Interview_Guide_Technical_Operations.docx
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/28_Interview_Guide_Business_Users.docx
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/29_Court_Completion_Signoff.docx
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/30_QA_Audit_Spot-Check_Procedures.docx
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/31_Risks_Issues_Log_Discovery.docx
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/32_Automation_Runbook_Collector_Setup_AWS_.docx
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/33_Automation_Runbook_Collector_Setup_Azure_.docx
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/34_Automation_Runbook_Collector_Setup_GCP_.docx
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/35_Automation_Runbook_Collector_Setup_OCI_.docx
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/36_API_Exports_Specification.docx
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/37_Dashboards_Reporting_Specification.docx
CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/38_Master_Index_of_Court_Binders.docx

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Page 93 of 117

CCoE_Build_Kit_v1_300Courts/50_DISCOVERY_INVENTORY/ZZ_Index_of_Documents.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/00_Cover_Sheet.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/01_Terminology_and_Acronyms.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/02_Migration_Factory_Operating_Model.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/02_Wave_Plan.csv
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/03_Cutover_Runbook.md
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/03_Roles_and_RACI.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/04_Court_Onboarding_Intake.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/04_VMware_to_Cloud.md
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/05_Wave_Planning_Scheduling_Playbook.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/06_Environment_Strategy_Promotion.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/07_Data_Migration_Strategy.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/08_Application_Migration_Rehost_Lift-and-Shift_.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/09_Application_Migration_Replatform.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/10_Application_Migration_Refactor.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/11_Application_Migration_Repurchase_SaaS_.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/12_Application_Disposition_Retire_Retain.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/13_Cutover_Validation_Runbook.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/14_Rollback_Backout_Strategy.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/15_Performance_Load_Test_Plan.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/16_Security_Validation_ATO_Evidence_During_Migration_.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/17_DR_Failover_Test_Procedure_per_Wave.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/18_Tagging_Governance_Post-Migration.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/19_CI_CD_Release_Management_Integration.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/20_Automation_Toolchain_Orchestration.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/21_Observability_Onboarding.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/22_Hypercare_Plan.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/23_Knowledge_Transfer_Handoff.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/24_FinOps_Controls_for_Migration.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/25_Change_Management_Training_Execution.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/26_Quality_Gates_Entry_Exit.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/27_Court_Execution_Binder_Template.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/28_RAID_Factory.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/29_Evidence_Collection_Pre_During_Post_Cutover.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/50_AWS_AWS_Database_Migration_Patterns.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/50_AWS_AWS_Network_Cutover_Patterns.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/50_AWS_AWS_PaaS_Adoption_Patterns.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/50_AWS_AWS_VMware-to-Cloud_Runbook.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/60_Azure_Azure_Database_Migration_Patterns.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/60_Azure_Azure_Network_Cutover_Patterns.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/60_Azure_Azure_PaaS_Adoption_Patterns.docx

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Page 94 of 117

CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/60_Azure_Azure_VMware-to-Cloud_Runbook.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/70_GCP_GCP_Database_Migration_Patterns.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/70_GCP_GCP_Network_Cutover_Patterns.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/70_GCP_GCP_PaaS_Adoption_Patterns.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/70_GCP_GCP_VMware-to-Cloud_Runbook.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/80_OCI_OCI_Database_Migration_Patterns.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/80_OCI_OCI_Network_Cutover_Patterns.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/80_OCI_OCI_PaaS_Adoption_Patterns.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/80_OCI_OCI_VMware-to-Cloud_Runbook.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/99_Index_of_Documents.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/ANNEX_User_Uploaded/
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/ANNEX_User_Uploaded/01_Factory_Overview.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/ANNEX_User_Uploaded/03_Cutover_Runbook.docx
CCoE_Build_Kit_v1_300Courts/60_MIGRATION_FACTORY/ANNEX_User_Uploaded/04_VMware_to_Cloud.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/00_Cover_Sheet.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/01_Terminology_and_Acronyms.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/02_AWS_Landing_Zone_Overview_Principles.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/03_Court_Isolation_Cross-Tenant_Access_Model.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/04_Organizations_Structure_OU_Design.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/05_Account_Vending_Lifecycle_AVM_.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/06_SCP_Catalog.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/07_AWS_Config_Conformance_Packs.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/08_Identity_Federation_Role_Catalog.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/09_Logging_Monitoring_SIEM_Integration.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/10_KMS_Key_Management.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/11_Network_Baseline_VPC_TGW_Ingress_Egress.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/12_Private_Service_Access_Patterns_PrivateLink_.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/13_Baseline_Security_Services.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/14_Tagging_Metadata_Standard.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/15_Backup_Restore_DR_Baselines.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/16_Vulnerability_Patch_Inspector_SSM_.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/17_Configuration_Management_Images.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/18_FinOps_Controls_Budgets.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/19_Change_Control_Infra_Pipelines_CI_CD_.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/20_Validation_Audit_Checklists.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/21_ATO_Inheritance_Evidence_Map_AWS_LZ_.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/22_AWS_IaaS_Standards_Baselines_LZ_.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/23_AWS_PaaS_Patterns_Guardrails_LZ_.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/24_AWS_SaaS_Integration_Governance_LZ_.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/99_Index_of_Documents.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/ANNEX_User_Uploaded/

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Page 95 of 117

CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/ANNEX_User_Uploaded/00_Cover_Sheet.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/ANNEX_User_Uploaded/00_Readme.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/ANNEX_User_Uploaded/01_Terminology_and_Acronyms.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/ANNEX_User_Uploaded/02_AWS_Landing_Zone_Overview_Principles.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/ANNEX_User_Uploaded/02_Reference_Architecture.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/ANNEX_User_Uploaded/03_Guardrails_and_Policies.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/ANNEX_User_Uploaded/03_Organizations_Structure_OU_Design.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/ANNEX_User_Uploaded/04_Account_Vending_Lifecycle_AVM_.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/ANNEX_User_Uploaded/04_CICD_Pipelines.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/ANNEX_User_Uploaded/05_SCP_Catalog.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/ANNEX_User_Uploaded/06_AWS_Config_Conformance_Packs.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/ANNEX_User_Uploaded/07_Identity_Federation_Role_Catalog.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/ANNEX_User_Uploaded/08_Logging_Monitoring_SIEM_Integration.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/ANNEX_User_Uploaded/09_KMS_Key_Management.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/ANNEX_User_Uploaded/10_Network_Baseline_VPC_TGW_Ingress_Egress.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/ANNEX_User_Uploaded/11_Private_Service_Access_Patterns_PrivateLink_.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/ANNEX_User_Uploaded/12_Baseline_Security_Services.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/ANNEX_User_Uploaded/13_Tagging_Metadata_Standard.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/ANNEX_User_Uploaded/14_Backup_Restore_DR_Baselines.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/ANNEX_User_Uploaded/15_Vulnerability_Patch_Inspector_SSM_.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/ANNEX_User_Uploaded/16_Configuration_Management_Images.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/ANNEX_User_Uploaded/17_FinOps_Controls_Budgets.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/ANNEX_User_Uploaded/18_Change_Control_Infra_Pipelines_CI_CD_.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/ANNEX_User_Uploaded/19_Validation_Audit_Checklists.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/ANNEX_User_Uploaded/20_ATO_Inheritance_Evidence_Map_AWS_LZ_.docx

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Page 96 of 117

CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/ANNEX_User_Uploaded/21_Runbook_Create_Org_CloudTrail_Central_Log_Archive.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/ANNEX_User_Uploaded/22_Runbook_Court_Account_Creation_AVM_.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/ANNEX_User_Uploaded/23_Runbook_Enable_GuardDuty_SecurityHub_Macie_Detective_Inspector.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/ANNEX_User_Uploaded/24_Runbook_Conformance_Packs_Auto_Remediation.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/ANNEX_User_Uploaded/25_Runbook_VPC_TGW_Baseline_per_Court.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/ANNEX_User_Uploaded/99_Index_of_Documents.docx
CCoE_Build_Kit_v1_300Courts/70_AWS_LANDING_ZONE/__tmp.docx
CCoE_Build_Kit_v1_300Courts/71_AZURE_LANDING_ZONE/
CCoE_Build_Kit_v1_300Courts/71_AZURE_LANDING_ZONE/00_Cover_Sheet.docx
CCoE_Build_Kit_v1_300Courts/71_AZURE_LANDING_ZONE/01_BOM.csv
CCoE_Build_Kit_v1_300Courts/71_AZURE_LANDING_ZONE/01_Terminology_and_Acronyms.docx
CCoE_Build_Kit_v1_300Courts/71_AZURE_LANDING_ZONE/02_Azure_Landing_Zone_Overview_Principles.docx
CCoE_Build_Kit_v1_300Courts/71_AZURE_LANDING_ZONE/03_Court_Isolation_Cross-Tenant_Access_Model.docx
CCoE_Build_Kit_v1_300Courts/71_AZURE_LANDING_ZONE/04_Management_Group_Structure_Subscription_Design.docx
CCoE_Build_Kit_v1_300Courts/71_AZURE_LANDING_ZONE/05_Subscription_Vending_Lifecycle.docx
CCoE_Build_Kit_v1_300Courts/71_AZURE_LANDING_ZONE/06_Policy_Catalog_Azure_Policy_Initiatives_.docx
CCoE_Build_Kit_v1_300Courts/71_AZURE_LANDING_ZONE/07_Defender_for_Cloud_Compliance_Packs.docx
CCoE_Build_Kit_v1_300Courts/71_AZURE_LANDING_ZONE/08_Entra_ID_Federation_Role_Catalog.docx
CCoE_Build_Kit_v1_300Courts/71_AZURE_LANDING_ZONE/09_Logging_Monitoring_and_Sentinel_Integration.docx
CCoE_Build_Kit_v1_300Courts/71_AZURE_LANDING_ZONE/10_Key_Vault_Managed_HSM_Key_Management.docx
CCoE_Build_Kit_v1_300Courts/71_AZURE_LANDING_ZONE/11_Network_Baseline_vWAN_Hub-Spoke_Ingress_Egress.docx
CCoE_Build_Kit_v1_300Courts/71_AZURE_LANDING_ZONE/12_Private_Link_Service_Access_Patterns.docx
CCoE_Build_Kit_v1_300Courts/71_AZURE_LANDING_ZONE/13_Baseline_Security_Services.docx
CCoE_Build_Kit_v1_300Courts/71_AZURE_LANDING_ZONE/14_Tagging_Metadata_Standard.docx
CCoE_Build_Kit_v1_300Courts/71_AZURE_LANDING_ZONE/15_Backup_Restore_DR_Baselines.docx
CCoE_Build_Kit_v1_300Courts/71_AZURE_LANDING_ZONE/16_Vulnerability_Patch_Management.docx
CCoE_Build_Kit_v1_300Courts/71_AZURE_LANDING_ZONE/17_Configuration_Management_Images.docx
CCoE_Build_Kit_v1_300Courts/71_AZURE_LANDING_ZONE/18_FinOps_Controls_Budgets.docx
CCoE_Build_Kit_v1_300Courts/71_AZURE_LANDING_ZONE/19_Change_Control_Infrastructure_Pipelines_CI_CD_.docx
CCoE_Build_Kit_v1_300Courts/71_AZURE_LANDING_ZONE/20_Validation_Audit_Checklists.docx
CCoE_Build_Kit_v1_300Courts/71_AZURE_LANDING_ZONE/21_ATO_Inheritance_Evidence_Map_Azure_LZ_.docx
CCoE_Build_Kit_v1_300Courts/71_AZURE_LANDING_ZONE/22_Azure_IaaS_Standards_Baselines_LZ_.docx

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Page 97 of 117

CCoE_Build_Kit_v1_300Courts/71_AZURE_LANDING_ZONE/23_Azure_PaaS_Patterns_Guardrails_LZ_.docx
CCoE_Build_Kit_v1_300Courts/71_AZURE_LANDING_ZONE/24_Azure_SaaS_Integration_Governance_LZ_.docx
CCoE_Build_Kit_v1_300Courts/71_AZURE_LANDING_ZONE/25_Runbook_Create_Central_Log_Analytics_Diagnostic_Settings.docx
CCoE_Build_Kit_v1_300Courts/71_AZURE_LANDING_ZONE/26_Runbook_Subscription_Creation_via_AVM_Automation.docx
CCoE_Build_Kit_v1_300Courts/71_AZURE_LANDING_ZONE/27_Runbook_Enable_Defender_Plans_Sentinel.docx
CCoE_Build_Kit_v1_300Courts/71_AZURE_LANDING_ZONE/28_Runbook_Policy_Initiatives_Auto-Remediation.docx
CCoE_Build_Kit_v1_300Courts/71_AZURE_LANDING_ZONE/29_Runbook_vWAN_Hub-Spoke_Baseline_per_Court.docx
CCoE_Build_Kit_v1_300Courts/71_AZURE_LANDING_ZONE/99_Index_of_Documents.docx
CCoE_Build_Kit_v1_300Courts/71_AZURE_LANDING_ZONE/ANNEX_User_Uploaded/
CCoE_Build_Kit_v1_300Courts/71_AZURE_LANDING_ZONE/ANNEX_User_Uploaded/00_Readme.docx
CCoE_Build_Kit_v1_300Courts/71_AZURE_LANDING_ZONE/ANNEX_User_Uploaded/02_Reference_Architecture.docx
CCoE_Build_Kit_v1_300Courts/71_AZURE_LANDING_ZONE/ANNEX_User_Uploaded/03_Guardrails_and_Policies.docx
CCoE_Build_Kit_v1_300Courts/71_AZURE_LANDING_ZONE/ANNEX_User_Uploaded/04_CICD_Pipelines.docx
CCoE_Build_Kit_v1_300Courts/72_GCP_LANDING_ZONE/
CCoE_Build_Kit_v1_300Courts/72_GCP_LANDING_ZONE/00_Cover_Sheet.docx
CCoE_Build_Kit_v1_300Courts/72_GCP_LANDING_ZONE/01_BOM.csv
CCoE_Build_Kit_v1_300Courts/72_GCP_LANDING_ZONE/01_Terminology_and_Acronyms.docx
CCoE_Build_Kit_v1_300Courts/72_GCP_LANDING_ZONE/02_GCP_Landing_Zone_Overview_Principles.docx
CCoE_Build_Kit_v1_300Courts/72_GCP_LANDING_ZONE/03_Court_Isolation_Cross-Tenant_Access_Model.docx
CCoE_Build_Kit_v1_300Courts/72_GCP_LANDING_ZONE/04_Folder_Structure_Project_Design.docx
CCoE_Build_Kit_v1_300Courts/72_GCP_LANDING_ZONE/05_Project_Vending_Lifecycle.docx
CCoE_Build_Kit_v1_300Courts/72_GCP_LANDING_ZONE/06_Organization_Policy_Catalog.docx
CCoE_Build_Kit_v1_300Courts/72_GCP_LANDING_ZONE/07_SCC_Posture_Compliance_Packs.docx
CCoE_Build_Kit_v1_300Courts/72_GCP_LANDING_ZONE/08_Identity_Federation_Role_Catalog.docx
CCoE_Build_Kit_v1_300Courts/72_GCP_LANDING_ZONE/09_Logging_Monitoring_and_SIEM_Integration.docx
CCoE_Build_Kit_v1_300Courts/72_GCP_LANDING_ZONE/10_Cloud_KMS_Key_Management.docx
CCoE_Build_Kit_v1_300Courts/72_GCP_LANDING_ZONE/11_Network_Baseline_VPC_Ingress_Egress.docx
CCoE_Build_Kit_v1_300Courts/72_GCP_LANDING_ZONE/12_Private_Service_Connect_Access_Patterns.docx
CCoE_Build_Kit_v1_300Courts/72_GCP_LANDING_ZONE/13_Baseline_Security_Services.docx
CCoE_Build_Kit_v1_300Courts/72_GCP_LANDING_ZONE/14_Tagging_Metadata_Standard.docx
CCoE_Build_Kit_v1_300Courts/72_GCP_LANDING_ZONE/15_Backup_Restore_DR_Baselines.docx
CCoE_Build_Kit_v1_300Courts/72_GCP_LANDING_ZONE/16_Vulnerability_Patch_Management.docx
CCoE_Build_Kit_v1_300Courts/72_GCP_LANDING_ZONE/17_Configuration_Management_Images.docx
CCoE_Build_Kit_v1_300Courts/72_GCP_LANDING_ZONE/18_FinOps_Controls_Budgets.docx
CCoE_Build_Kit_v1_300Courts/72_GCP_LANDING_ZONE/19_Change_Control_Infrastructure_Pipelines_CI_CD_.docx
CCoE_Build_Kit_v1_300Courts/72_GCP_LANDING_ZONE/20_Validation_Audit_Checklists.docx

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Page 98 of 117

CCoE_Build_Kit_v1_300Courts/72_GCP_LANDING_ZONE/21_ATO_Inheritance_Evidence_Map_GCP_LZ_.docx
CCoE_Build_Kit_v1_300Courts/72_GCP_LANDING_ZONE/22_GCP_IaaS_Standards_Baselines_LZ_.docx
CCoE_Build_Kit_v1_300Courts/72_GCP_LANDING_ZONE/23_GCP_PaaS_Patterns_Guardrails_LZ_.docx
CCoE_Build_Kit_v1_300Courts/72_GCP_LANDING_ZONE/24_GCP_SaaS_Integration_Governance_LZ_.docx
CCoE_Build_Kit_v1_300Courts/72_GCP_LANDING_ZONE/25_Runbook_Centralized_Log_Sinks_Aggregation.docx
CCoE_Build_Kit_v1_300Courts/72_GCP_LANDING_ZONE/26_Runbook_Project_Creation_via_Automation.docx
CCoE_Build_Kit_v1_300Courts/72_GCP_LANDING_ZONE/27_Runbook_SCC_Posture_Enablement.docx
CCoE_Build_Kit_v1_300Courts/72_GCP_LANDING_ZONE/28_Runbook_Org_Policy_Auto-Remediation.docx
CCoE_Build_Kit_v1_300Courts/72_GCP_LANDING_ZONE/29_Runbook_VPC_Private_Service_Connect_per_Court.docx
CCoE_Build_Kit_v1_300Courts/72_GCP_LANDING_ZONE/99_Index_of_Documents.docx
CCoE_Build_Kit_v1_300Courts/73_OCI_LANDING_ZONE/
CCoE_Build_Kit_v1_300Courts/73_OCI_LANDING_ZONE/00_Cover_Sheet.docx
CCoE_Build_Kit_v1_300Courts/73_OCI_LANDING_ZONE/01_BOM.csv
CCoE_Build_Kit_v1_300Courts/73_OCI_LANDING_ZONE/01_Terminology_and_Acronyms.docx
CCoE_Build_Kit_v1_300Courts/73_OCI_LANDING_ZONE/02_OCI_Landing_Zone_Overview_Principles.docx
CCoE_Build_Kit_v1_300Courts/73_OCI_LANDING_ZONE/03_Court_Isolation_Cross-Tenant_Access_Model.docx
CCoE_Build_Kit_v1_300Courts/73_OCI_LANDING_ZONE/04_Compartment_Structure_Tenancy_Design.docx
CCoE_Build_Kit_v1_300Courts/73_OCI_LANDING_ZONE/05_Compartment_Provisioning_Lifecycle.docx
CCoE_Build_Kit_v1_300Courts/73_OCI_LANDING_ZONE/06_Security_Zones_Policy_Catalog.docx
CCoE_Build_Kit_v1_300Courts/73_OCI_LANDING_ZONE/07_Cloud_Guard_Recipes_Compliance_Packs.docx
CCoE_Build_Kit_v1_300Courts/73_OCI_LANDING_ZONE/08_Federation_IAM_Policies_Catalog.docx
CCoE_Build_Kit_v1_300Courts/73_OCI_LANDING_ZONE/09_Logging_Monitoring_and_SIEM_Integration.docx
CCoE_Build_Kit_v1_300Courts/73_OCI_LANDING_ZONE/10_Vault_KMS_Key_Management.docx
CCoE_Build_Kit_v1_300Courts/73_OCI_LANDING_ZONE/11_Network_Baseline_VCN_Ingress_Egress.docx
CCoE_Build_Kit_v1_300Courts/73_OCI_LANDING_ZONE/12_Service_Gateway_Private_Endpoint_Patterns.docx
CCoE_Build_Kit_v1_300Courts/73_OCI_LANDING_ZONE/13_Baseline_Security_Services.docx
CCoE_Build_Kit_v1_300Courts/73_OCI_LANDING_ZONE/14_Tagging_Metadata_Standard.docx
CCoE_Build_Kit_v1_300Courts/73_OCI_LANDING_ZONE/15_Backup_Restore_DR_Baselines.docx
CCoE_Build_Kit_v1_300Courts/73_OCI_LANDING_ZONE/16_Vulnerability_Patch_Management.docx
CCoE_Build_Kit_v1_300Courts/73_OCI_LANDING_ZONE/17_Configuration_Management_Images.docx
CCoE_Build_Kit_v1_300Courts/73_OCI_LANDING_ZONE/18_FinOps_Controls_Budgets.docx
CCoE_Build_Kit_v1_300Courts/73_OCI_LANDING_ZONE/19_Change_Control_Infrastructure_Pipelines_CI_CD_.docx
CCoE_Build_Kit_v1_300Courts/73_OCI_LANDING_ZONE/20_Validation_Audit_Checklists.docx
CCoE_Build_Kit_v1_300Courts/73_OCI_LANDING_ZONE/21_ATO_Inheritance_Evidence_Map_OCI_LZ_.docx
CCoE_Build_Kit_v1_300Courts/73_OCI_LANDING_ZONE/22_OCI_IaaS_Standards_Baselines_LZ_.docx
CCoE_Build_Kit_v1_300Courts/73_OCI_LANDING_ZONE/23_OCI_PaaS_Patterns_Guardrails_LZ_.docx
CCoE_Build_Kit_v1_300Courts/73_OCI_LANDING_ZONE/24_OCI_SaaS_Integration_Governance_LZ_.docx
CCoE_Build_Kit_v1_300Courts/73_OCI_LANDING_ZONE/25_Runbook_Central_Logging_Service_Connectors.docx
CCoE_Build_Kit_v1_300Courts/73_OCI_LANDING_ZONE/26_Runbook_Compartment_Provisioning_Automation.docx
CCoE_Build_Kit_v1_300Courts/73_OCI_LANDING_ZONE/27_Runbook_Cloud_Guard_Posture_Enablement.docx

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Page 99 of 117

CCoE_Build_Kit_v1_300Courts/73_OCI_LANDING_ZONE/28_Runbook_Security_Zones_Auto-Remediation.docx
CCoE_Build_Kit_v1_300Courts/73_OCI_LANDING_ZONE/29_Runbook_VCN_Service_Gateway_per_Court.docx
CCoE_Build_Kit_v1_300Courts/73_OCI_LANDING_ZONE/99_Index_of_Documents.docx
CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/
CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/00_Cover_Sheet.docx
CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/01_Terminology_and_Acronyms.docx
CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/02_Cross-Cloud_Vision_Principles.docx
CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/03_Cloud_Selection_Method_Weighted_Decision_Matrix.docx
CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/03_Selection_Scoring_Template.csv
CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/04_Common_Governance_Operating_Model_CCoE_.docx
CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/05_Role_Catalog_RBAC_ABAC_Taxonomy.docx
CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/06_Policy-as-Code_Framework_Multi-Cloud.docx
CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/07_Tagging_Metadata_Harmonization.docx
CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/08_Identity_Federation_Standard.docx
CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/09_Secrets_Key_Management_Standard.docx
CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/10_Network_Reference_Patterns_Private-First_.docx
CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/11_Private_Service_Access_PLA_PSC_SG_.docx
CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/12_Logging_Telemetry_Normalization.docx
CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/13_SIEM_SOAR_Integration_Multi-Cloud.docx
CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/14_Vulnerability_Patch_Management_Harmonized.docx
CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/15_STIG_CIS_Baseline_Harmonization.docx
CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/16_Container_Kubernetes_Baselines.docx
CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/17_Serverless_Baselines.docx
CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/18_Data_Protection_DLP.docx
CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/19_Backup_DR_Resilience_Patterns.docx
CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/20_SaaS_Integration_Governance.docx
CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/21_CJIS_Privacy_Considerations.docx
CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/22_ConMon_Control_Evidence_Common_Plan.docx
CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/23_Control_Mapping_NIST_SP_800-53_Rev._5_FedRAMP.docx
CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/24_FinOps_Cross_Cloud.docx
CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/25_Software_Supply_Chain_SLSA_SBOM_Common.docx
CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/26_CI_CD_Standards_Multi_Cloud.docx
CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/27_Quality_Gates_KPIs.docx
CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/28_Training_Change_Management.docx
CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/29_Court_Onboarding_to_CCoE_Checklist.docx
CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/30_Runbooks_Index.docx

CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/31_Runbook_Standardize_Tags_Labels_Across_Clouds.docx
CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/32_Runbook_Connect_Cloud_Logs_to_Central_SIEM.docx
CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/33_Runbook_Court_Onboarding_to_CCoE.docx
CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/34_Runbook_Enable_Common_Compliance_Packs.docx
CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/35_Runbook_Backup_DR_Drill_Scheduling_Cross_Cloud_.docx
CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/36_Runbook_Secret_Rotation_Program.docx
CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/37_Runbook_ATO_Evidence_Exports_ConMon_Jobs.docx
CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/99_Index_of_Documents.docx
CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/ANNEX_User_Uploaded/
CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/ANNEX_User_Uploaded/01_Common_Services.docx
CCoE_Build_Kit_v1_300Courts/74_CROSS_CLOUD_COMMONS/ANNEX_User_Uploaded/02_Provider_Selection_Framework.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/00_Cover_Sheet.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/01_Terminology_and_Acronyms.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/02_DevSecOps_Vision_Principles.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/03_Operating_Model_Roles_RACI_.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/04_SDLC_Policy_Lifecycle.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/05_Branching_Strategy_Protections.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/06_Secure_Coding_Standard_Language-Agnostic_.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/07_Threat_Modeling_Standard.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/08_Golden_Pipeline_Patterns_Matrix.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/09_Source_Control_Governance.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/10_Identity_Access_for_Dev_Tooling.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/11_Secrets_Management_in_Build_Runtime.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/12_Dependency_Supply_Chain_Security.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/13_Build_Artifact_Signing_Provenance.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/14_Container_Build_Standard.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/15_Kubernetes_Release_Standard.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/16_Infrastructure-as-Code_Standard.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/17_Policy-as-Code_in_CI.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/18_Testing_Strategy_Unit_E2E_Security_.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/19_SAST_SCA_DAST_IAST_Configuration.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/20_Open_Source_License_Compliance.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/21_Quality_Release_Gates.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/22_Environment_Promotion_Change_Control.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/23_Progressive_Delivery_Patterns.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/24_Observability_SLOs_Error_Budgets.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/25_Incident_Management_in_DevOps.docx

CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/26_Vulnerability_Management_in_Pipelines.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/27_Code_Review_Pairing_Practices.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/28_Security_Champions_Program.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/29_Training_Secure_Code_Curriculum.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/30_Evidence_Capture_ATO_Alignment.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/31_Metrics_KPIs_DORA_Security_.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/32_Continuous_Improvement_Backlog.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/33_Tooling_Reference_Mapping_per_CI_CD_platform_.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/34_Golden_Pipeline_Template_Web_App_Node_React_.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/35_Golden_Pipeline_Template_API_Python_Flask_.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/36_Golden_Pipeline_Template_Container_Service_Kubernetes_ .docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/37_Golden_Pipeline_Template_IaC_Terraform_.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/38_Golden_Pipeline_Template_Data_ETL_dbt_Airflow_.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/39_PR_Release_Checklist.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/40_Change_Ticket_Template_for_CCB_.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/41_Emergency_Fix_Hotfix_Runbook.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/42_Rollback_Runbook.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/43_SBOM_Generation_Storage_Procedure.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/44_Cosign_Sigstore_Keyless_Signing_Procedure.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/45_Third_Party_Risk_for_OSS_Dependencies.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/46_IDE_Security_Plugins_Standard.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/47_Pre_commit_Hooks_Standard.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/48_Artifact_Repository_Governance.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/49_Container_Registry_Governance.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/50_Image_Promotion_Strategy.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/51_Runtime_Controls_Admission_Runtime_Scanning.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/52_Secrets_Scanning_Program.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/53_Compliance_Control_Mapping_DevSecOps.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/54_Evidence_Index_Storage_Locations.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/99_Index_of_Documents.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/ANNEX_User_Uploaded/
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/ANNEX_User_Uploaded/01_Software_Factory.docx
CCoE_Build_Kit_v1_300Courts/80_DEVSECOPS/ANNEX_User_Uploaded/02_Policy_Gates.docx
CCoE_Build_Kit_v1_300Courts/81_CICD/
CCoE_Build_Kit_v1_300Courts/81_CICD/00_Cover_Sheet.docx
CCoE_Build_Kit_v1_300Courts/81_CICD/01_Terminology_and_Acronyms.docx
CCoE_Build_Kit_v1_300Courts/81_CICD/02_CI_CD_Vision_Principles.docx
CCoE_Build_Kit_v1_300Courts/81_CICD/03_Operating_Model_Roles_RACI_.docx
CCoE_Build_Kit_v1_300Courts/81_CICD/04_SDLC_Policy_Lifecycle.docx
CCoE_Build_Kit_v1_300Courts/81_CICD/05_Branch_Protection_Merge_Strategy.docx
CCoE_Build_Kit_v1_300Courts/81_CICD/06_Golden_Pipeline_Stage_Matrix.docx
CCoE_Build_Kit_v1_300Courts/81_CICD/07_Testing_Strategy_Integration.docx
CCoE_Build_Kit_v1_300Courts/81_CICD/08_Secrets_Identity_in_CI.docx
CCoE_Build_Kit_v1_300Courts/81_CICD/09_Artifact_Signing_Provenance.docx

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Page 102 of 117

CCoE_Build_Kit_v1_300Courts/81_CICD/10_SBOM_Standard_Storage.docx
CCoE_Build_Kit_v1_300Courts/81_CICD/11_Policy-as-Code_Enforcement.docx
CCoE_Build_Kit_v1_300Courts/81_CICD/12_Environment_Promotion_Release_Management.docx
CCoE_Build_Kit_v1_300Courts/81_CICD/13_Deployment_Strategies.docx
CCoE_Build_Kit_v1_300Courts/81_CICD/14_Rollback_Backout_Strategy.docx
CCoE_Build_Kit_v1_300Courts/81_CICD/15_Evidence_Capture_ATO_Alignment.docx
CCoE_Build_Kit_v1_300Courts/81_CICD/16_Metrics_KPIs_DORA_Security_.docx
CCoE_Build_Kit_v1_300Courts/81_CICD/17_Tooling_Reference_Mapping_per_CI_CD_platform_.docx
CCoE_Build_Kit_v1_300Courts/81_CICD/18_Monorepo_vs_Polyrepo_Strategy.docx
CCoE_Build_Kit_v1_300Courts/81_CICD/19_GitHub_Actions_OIDC_to_AWS_Azure_GCP_OCI.docx
CCoE_Build_Kit_v1_300Courts/81_CICD/20_Azure_DevOps_Pipelines_Federated_Credentials.docx
CCoE_Build_Kit_v1_300Courts/81_CICD/21_GitLab_CI_Workload_Identity_Runners.docx
CCoE_Build_Kit_v1_300Courts/81_CICD/22_GCP_Cloud_Build_Workload_Identity_Federation.docx
CCoE_Build_Kit_v1_300Courts/81_CICD/23_AWS_CodePipeline_CodeBuild_Cross-Account_Roles.docx
CCoE_Build_Kit_v1_300Courts/81_CICD/24_Golden_Pipeline_Template_Web_App_Node_React_.docx
CCoE_Build_Kit_v1_300Courts/81_CICD/25_Golden_Pipeline_Template_API_Python_Flask_.docx
CCoE_Build_Kit_v1_300Courts/81_CICD/26_Golden_Pipeline_Template_Container_Service_Kubernetes_.docx
CCoE_Build_Kit_v1_300Courts/81_CICD/27_Golden_Pipeline_Template_IaC_Terraform_.docx
CCoE_Build_Kit_v1_300Courts/81_CICD/28_Golden_Pipeline_Template_Data_ETL_dbt_Airflow_.docx
CCoE_Build_Kit_v1_300Courts/81_CICD/29_Runbook_Secure_Runners_Agents.docx
CCoE_Build_Kit_v1_300Courts/81_CICD/30_Runbook_Connect_CI_to_Artifact_Repositories.docx
CCoE_Build_Kit_v1_300Courts/81_CICD/31_Runbook_Ephemeral_Environments_for_PRs.docx
CCoE_Build_Kit_v1_300Courts/81_CICD/32_Runbook_Key_Secret_Rotation_in_Pipelines.docx
CCoE_Build_Kit_v1_300Courts/81_CICD/33_Runbook_Break-Glass_Pipeline_Procedure.docx
CCoE_Build_Kit_v1_300Courts/81_CICD/34_Runbook_Pipeline_DR_Backup.docx
CCoE_Build_Kit_v1_300Courts/81_CICD/35_Runbook_Nightly_Deep_Security_Scans.docx
CCoE_Build_Kit_v1_300Courts/81_CICD/99_Index_of_Documents.docx
CCoE_Build_Kit_v1_300Courts/81_CICD/ANNEX_User_Uploaded/
CCoE_Build_Kit_v1_300Courts/81_CICD/ANNEX_User_Uploaded/01_Pipelines.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/
CCoE_Build_Kit_v1_300Courts/82_AI_ML/00_Cover_Sheet.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/01_Terminology_and_Acronyms.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/02_AI_ML_Vision_Principles_for_the_Judiciary.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/03_Responsible_AI_Governance_Cross_Cloud_.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/04_MLOps_Operating_Model_Roles_RACI_.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/05_Model_Lifecycle_Policy.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/06_Data_Governance_for_AI.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/07_Feature_Store_Lineage_Standards.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/08_Training_Data_Management_Quality.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/09_Model_Registry_Promotion_Workflow.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/10_Model_Evaluation_Risk_Scoring_Standard.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/11_Bias_Fairness_Accessibility_Testing_Protocol.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/12_Robustness_Safety_Adversarial_Testing.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/13_GenAI_Guardrails_RAG_Standard.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/14_Security_Controls_for_AI_Systems.docx

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Page 103 of 117

CCoE_Build_Kit_v1_300Courts/82_AI_ML/15_Monitoring_Drift_Feedback_Management.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/16_Incident_Response_for_AI_Systems.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/17_FinOps_for_AI_GPU_TPU_Inferencing_.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/18_Procurement_Third_Party_Model_Due_Diligence.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/19_eDiscovery_Records_for_AI.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/20_ATO_Evidence_Map_AI_Systems.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/21_AWS_Reference_Architecture_AWS_SageMaker_Bedrock_Private_Access_.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/22_AWS_IaaS_PaaS_SaaS_Overlays_AWS_AI.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/23_Azure_Reference_Architecture_Azure_Azure_ML_Azure_OpenAI_Private_Link_.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/24_Azure_IaaS_PaaS_SaaS_Overlays_Azure_AI.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/25_GCP_Reference_Architecture_GCP_Vertex_AI_Private_Service_Connect_.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/26_GCP_IaaS_PaaS_SaaS_Overlays_GCP_AI.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/27_OCI_Reference_Architecture_OCI_Data_Science_Generative_AI_Service_.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/28_OCI_IaaS_PaaS_SaaS_Overlays_OCI_AI.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/29_Template_Model_Card.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/30_Template_Data_Card.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/31_Template_System_Card.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/32_Template_DPIA_PIA_AI_.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/33_Template_Evaluation_Plan_AI_GenAI_.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/34_Template_AI_System_Change_Ticket_Addendum.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/35_Runbook_Build_Private_AI_Environment_per_Court.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/36_Runbook_RAG_Setup_with_Court_Data.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/37_Runbook_Model_Deployment_Canary_Shadow_.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/38_Runbook_Red_Team_Exercise_GenAI_.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/39_Runbook_Drift_Detection_Response.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/40_Runbook_Key_Secret_Rotation_for_AI_Services.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/41_Runbook_Dataset_Versioning_Approval.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/42_Evidence_Index_&_Storage_Locations_AIML.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/99_Index_of_Documents.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/ANNEX_User_Uploaded/
CCoE_Build_Kit_v1_300Courts/82_AI_ML/ANNEX_User_Uploaded/01_AI_ML_Governance.docx
CCoE_Build_Kit_v1_300Courts/82_AI_ML/ANNEX_User_Uploaded/02_Platform_Options.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/00_Cover_Sheet.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/01_Terminology_and_Acronyms.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/02_Data_Platform_Vision_Principles.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/03_Operating_Model_Roles_RACI_.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/04_Reference_Architectures_Overview.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/05_Ingestion_Integration_Standard_Batch_Streaming_.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/06_Data_Catalog_Lineage_Discovery.docx

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Page 104 of 117

CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/07_Data_Governance_Policy.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/08_Data_Security_Privacy.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/09_Access_Model_RBAC_ABAC_Row_Column_Level_Security_.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/10_Key_Management_Secrets.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/11_Tagging_Metadata_Standard.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/12_Schema_Management_Evolution.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/13_Data_Quality_Observability.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/14_Master_Data_Management_MDM_Reference_Data.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/15_Data_Sharing_Contracts.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/16_Data_APIs_Domain_Data_Products.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/17_Streaming_Platform_Standard.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/18_Batch_Processing_Standard.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/19_Storage_Tiers_Lifecycle.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/20_Table_Formats_Governance.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/21_Warehouse_Standard.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/22_BI_Analytics_Standard.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/23_Migration_Playbook_Databases_Files.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/24_Retention_eDiscovery_Legal_Hold.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/25_Observability_Logging_for_Data_Platform.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/26_FinOps_for_Data_Platform.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/27_ATO_Inheritance_Control_Mapping_Data_Platform.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/28_AWS_Data_Platform_Reference_AWS.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/29_AWS_AWS_IaaS_PaaS_SaaS_Overlays_Data.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/30_AWS_AWS_Data_Protection_DLP.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/31_Azure_Data_Platform_Reference_Azure.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/32_Azure_Azure_IaaS_PaaS_SaaS_Overlays_Data.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/33_Azure_Azure_Data_Protection_DLP.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/34_GCP_Data_Platform_Reference_GCP.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/35_GCP_GCP_IaaS_PaaS_SaaS_Overlays_Data.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/36_GCP_GCP_Data_Protection_DLP.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/37_OCI_Data_Platform_Reference_OCI.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/38_OCI_OCI_IaaS_PaaS_SaaS_Overlays_Data.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/39_OCI_OCI_Data_Protection_DLP.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/40_Template_Data_Product_Charter.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/41_Template_Data_Contract.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/42_Template_Quality_Rules_Catalog.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/43_Template_Schema_Registry_Entry.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/44_Template_Access_Policy_RBAC_ABAC_.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/45_Template_Retention_Schedule.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/46_Runbook_Catalog_Lineage_Setup_per_Cloud.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/47_Runbook_Batch_Ingestion_Pipeline.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/48_Runbook_Streaming_Ingestion_Pipeline.docx

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/49_Runbook_Schema_Change_Handling.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/50_Runbook_Access_Request_Provisioning.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/51_Runbook_Backup_Restore_Drill_Lakehouse_Tables_.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/52_Runbook_DR_Failover_for_Data_Platform.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/53_Runbook_eDiscovery_Export.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/54_Runbook_Cost_Anomaly_Budget_Response.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/55_Runbook_Cross_Region_Replication.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/56_Evidence_Index_&_Storage_Locations_Data_Platform.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/99_Index_of_Documents.docx
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/ANNEX_User_Uploaded/
CCoE_Build_Kit_v1_300Courts/83_DATA_PLATFORM/ANNEX_User_Uploaded/01_Modern_Data_Stack.docx
CCoE_Build_Kit_v1_300Courts/84_FINOPS/
CCoE_Build_Kit_v1_300Courts/84_FINOPS/00_Cover_Sheet.docx
CCoE_Build_Kit_v1_300Courts/84_FINOPS/01_Terminology_and_Acronyms.docx
CCoE_Build_Kit_v1_300Courts/84_FINOPS/02_FinOps_Vision_Principles.docx
CCoE_Build_Kit_v1_300Courts/84_FINOPS/03_Operating_Model_Roles_RACI_.docx
CCoE_Build_Kit_v1_300Courts/84_FINOPS/04_Governance_Policy_Budgets_Alerts_Escalation.docx
CCoE_Build_Kit_v1_300Courts/84_FINOPS/05_Account_Billing_Structure_Multi_Cloud.docx
CCoE_Build_Kit_v1_300Courts/84_FINOPS/06_Tagging_Labeling_Standard_for_Cost_Allocation.docx
CCoE_Build_Kit_v1_300Courts/84_FINOPS/07_Shared_Services_Allocation_Chargeback_Showback_.docx
CCoE_Build_Kit_v1_300Courts/84_FINOPS/08_Budgets_Forecasting.docx
CCoE_Build_Kit_v1_300Courts/84_FINOPS/09_Anomaly_Detection_Response.docx
CCoE_Build_Kit_v1_300Courts/84_FINOPS/10_Commitment_Management_SP_RI_CUD_SUD_.docx
CCoE_Build_Kit_v1_300Courts/84_FINOPS/11_Rightsizing_Scheduling_Program.docx
CCoE_Build_Kit_v1_300Courts/84_FINOPS/12_Storage_Lifecycle_Data_Egress_Management.docx
CCoE_Build_Kit_v1_300Courts/84_FINOPS/13_Network_Cost_Controls.docx
CCoE_Build_Kit_v1_300Courts/84_FINOPS/14_AI_Accelerator_GPU_TPU_Cost_Management.docx
CCoE_Build_Kit_v1_300Courts/84_FINOPS/15_License_Marketplace_Spend.docx
CCoE_Build_Kit_v1_300Courts/84_FINOPS/16_FinOps_KPIs_Scorecards.docx
CCoE_Build_Kit_v1_300Courts/84_FINOPS/17_Monthly_Review_Packet_Template.docx
CCoE_Build_Kit_v1_300Courts/84_FINOPS/18_Quarterly_Planning_Savings_Registry.docx
CCoE_Build_Kit_v1_300Courts/84_FINOPS/19_ATO_Evidence_Map_FinOps.docx
CCoE_Build_Kit_v1_300Courts/84_FINOPS/20_AWS_AWS_FinOps_Reference_Tools.docx
CCoE_Build_Kit_v1_300Courts/84_FINOPS/21_AWS_AWS_Budgeting_Allocation_Patterns.docx
CCoE_Build_Kit_v1_300Courts/84_FINOPS/22_Azure_Azure_FinOps_Reference_Tools.docx
CCoE_Build_Kit_v1_300Courts/84_FINOPS/23_Azure_Azure_Budgeting_Allocation_Patterns.docx
CCoE_Build_Kit_v1_300Courts/84_FINOPS/24_GCP_GCP_FinOps_Reference_Tools.docx
CCoE_Build_Kit_v1_300Courts/84_FINOPS/25_GCP_GCP_Budgeting_Allocation_Patterns.docx
CCoE_Build_Kit_v1_300Courts/84_FINOPS/26_OCI_OCI_FinOps_Reference_Tools.docx
CCoE_Build_Kit_v1_300Courts/84_FINOPS/27_OCI_OCI_Budgeting_Allocation_Patterns.docx
CCoE_Build_Kit_v1_300Courts/84_FINOPS/28_Template_Court_Budget_Policy.docx
CCoE_Build_Kit_v1_300Courts/84_FINOPS/29_Template_Allocation_Matrix.docx
CCoE_Build_Kit_v1_300Courts/84_FINOPS/30_Template_Commitment_Purchase_Justification.docx

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Page 106 of 117

CCoE_Build_Kit_v1_300Courts/84_FINOPS/31_Template_Variance_Report.docx
CCoE_Build_Kit_v1_300Courts/84_FINOPS/32_Template_Court_Invoice_Chargeback_Showback_.docx
CCoE_Build_Kit_v1_300Courts/84_FINOPS/33_Template_FinOps_Charter.docx
CCoE_Build_Kit_v1_300Courts/84_FINOPS/34_Runbook_Court_Onboarding_to_FinOps.docx
CCoE_Build_Kit_v1_300Courts/84_FINOPS/35_Runbook_Monthly_Review_Cycle.docx
CCoE_Build_Kit_v1_300Courts/84_FINOPS/36_Runbook_Tagging_Remediation_Campaign.docx
CCoE_Build_Kit_v1_300Courts/84_FINOPS/37_Runbook_Rightsizing_Scheduling_Campaign.docx
CCoE_Build_Kit_v1_300Courts/84_FINOPS/38_Runbook_Commitment_Planning_Buy.docx
CCoE_Build_Kit_v1_300Courts/84_FINOPS/39_Runbook_Anomaly_Triage_Kill_Switch.docx
CCoE_Build_Kit_v1_300Courts/84_FINOPS/40_Runbook_Year_End_True_Up.docx
CCoE_Build_Kit_v1_300Courts/84_FINOPS/41_Runbook_GPU_Accelerator_Scheduling.docx
CCoE_Build_Kit_v1_300Courts/84_FINOPS/99_Index_of_Documents.docx
CCoE_Build_Kit_v1_300Courts/84_FINOPS/ANNEX_User_Uploaded/
CCoE_Build_Kit_v1_300Courts/84_FINOPS/ANNEX_User_Uploaded/01_Cost_Governance.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/00_Cover_Sheet.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/01_Terminology_and_Acronyms.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/02_ITSM_Vision_Principles.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/03_Operating_Model_Organization_ITSM_CCoE_.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/04_Service_Portfolio_Catalog_Standard.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/05_Service_Level_Management_SLAs_OLAs_UCs_.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/06_Incident_Management_Policy.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/07_Major_Incident_Management_Runbook.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/08_Problem_Management_Policy.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/09_Knowledge_Management_Standard.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/10_Request_Fulfillment_Policy.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/11_Change_Management_Policy.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/12_CAB_Charter.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/13_Emergency_Change_ECAB_Procedure.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/14_Release_Deployment_Management.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/15_Configuration_Management_Plan_CMP_Policy.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/16_CMDB_Governance_Data_Model.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/17_Asset_Management_HAM_SAM_Standard.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/18_Baseline_Control_Versioning.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/19_Standard_Changes_Library.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/20_Maintenance_Windows_Freeze_Calendar.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/21_Service_Continuity_DR_Interface.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/22_Availability_Capacity_Management.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/23_Observability_ITOM_Integration.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/24_ITSM_Security_Privacy_Interface.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/25_FedRAMP_Control_Mapping_ITSM_CMP.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/26_Evidence_Capture_Audit_Trails.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/27_Integrations_ServiceNow_Jira_Service_Management_BMC.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/28_AWS_Service_Management_Overlay.docx

CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/29_Azure_Service_Management_Overlay.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/30_GCP_Service_Management_Overlay.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/31_OCI_Service_Management_Overlay.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/32_Multi_Cloud_Standardized_Change_Types_Workflows.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/33_Runbook_Connect_Cloud_Telemetry_to_ITSM.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/34_Runbook_Automated_Change_with_Policy-as-Code.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/35_Runbook_CMDB_Population_from_Cloud.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/36_Runbook_Patch_Vulnerability_Flow.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/37_Runbook_Access_Request_JIT_Approvals.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/38_Runbook_Change_Calendar_Management.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/39_Template_Request_for_Change_RFC_.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/40_Template_Release_Plan_Backout.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/41_Template_Post_Implementation_Review_PIR_.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/42_Template_Major_Incident_Report.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/43_Template_Service_Catalog_Item.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/44_Template_SLA_Definition.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/45_Metrics_KPIs_ITSM.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/46_Quality_Gates_CAB_Checklist.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/47_ATO_Interface_Change_Control_Evidence_Exports.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/48_Control_Inheritance_Matrix_ITSM_Landing_Zones_Apps_.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/99_Index_of_Documents.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/ANNEX_User_Uploaded/
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/ANNEX_User_Uploaded/01_ITSM_Integration.docx
CCoE_Build_Kit_v1_300Courts/85_ITSM_CMP/ANNEX_User_Uploaded/02_CMP_Capabilities.docx
CCoE_Build_Kit_v1_300Courts/90_OPERATIONS/
CCoE_Build_Kit_v1_300Courts/90_OPERATIONS/00_Cover_Sheet.docx
CCoE_Build_Kit_v1_300Courts/90_OPERATIONS/01_Terminology_and_Acronyms.docx
CCoE_Build_Kit_v1_300Courts/90_OPERATIONS/02_Operations_Vision_Principles.docx
CCoE_Build_Kit_v1_300Courts/90_OPERATIONS/03_Operating_Model_Roles_NOC_SRE_Platform_SecOps_Interface_.docx
CCoE_Build_Kit_v1_300Courts/90_OPERATIONS/04_Service_Health_Model_SLIs_SLOs_Error_Budgets_.docx
CCoE_Build_Kit_v1_300Courts/90_OPERATIONS/05_Observability_Standard_Logs_Metrics_Traces_.docx
CCoE_Build_Kit_v1_300Courts/90_OPERATIONS/06_Alerting_Standards_Noise_Reduction.docx
CCoE_Build_Kit_v1_300Courts/90_OPERATIONS/07_On_Call_Charter_Escalation_Policy.docx
CCoE_Build_Kit_v1_300Courts/90_OPERATIONS/08_Incident_Command_System_ICS_Procedures.docx
CCoE_Build_Kit_v1_300Courts/90_OPERATIONS/09_Capacity_Performance_Management.docx
CCoE_Build_Kit_v1_300Courts/90_OPERATIONS/10_Patch_Vulnerability_Operations.docx
CCoE_Build_Kit_v1_300Courts/90_OPERATIONS/11_Backup_Restore_Operations.docx
CCoE_Build_Kit_v1_300Courts/90_OPERATIONS/12_Disaster_Recovery_DR_Operations_Runbook.docx
CCoE_Build_Kit_v1_300Courts/90_OPERATIONS/13_Business_Continuity_Runbook.docx
CCoE_Build_Kit_v1_300Courts/90_OPERATIONS/14_Job_Scheduling_Orchestration_Standard.docx
CCoE_Build_Kit_v1_300Courts/90_OPERATIONS/15_Change_Window_Operations_Freeze_Calendar.docx
CCoE_Build_Kit_v1_300Courts/90_OPERATIONS/16_Release_Operations_Cutover_Procedures.docx
CCoE_Build_Kit_v1_300Courts/90_OPERATIONS/17_Tenant_Isolation_Monitoring_Controls.docx

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Page 108 of 117

CCoE_Build_Kit_v1_300Courts/90_OPERATIONS/18_Data_Handling_in_Operations_IL5_IL6_like_rigor_.docx
CCoE_Build_Kit_v1_300Courts/90_OPERATIONS/19_Access_Operations_JIT_JEA_Certificates_Keys_.docx
CCoE_Build_Kit_v1_300Courts/90_OPERATIONS/20_Runbook_Quality_Safety_Checks.docx
CCoE_Build_Kit_v1_300Courts/90_OPERATIONS/21_Postmortem_Problem_Review_Ops_view_.docx
CCoE_Build_Kit_v1_300Courts/90_OPERATIONS/22_Operations_Metrics_KPIs.docx
CCoE_Build_Kit_v1_300Courts/90_OPERATIONS/23_Evidence_Capture_ATO_Alignment_Operations.docx
CCoE_Build_Kit_v1_300Courts/90_OPERATIONS/24_AWS_Operations_Overlay_AWS.docx
CCoE_Build_Kit_v1_300Courts/90_OPERATIONS/25_Azure_Operations_Overlay_Azure.docx
CCoE_Build_Kit_v1_300Courts/90_OPERATIONS/26_GCP_Operations_Overlay_GCP.docx
CCoE_Build_Kit_v1_300Courts/90_OPERATIONS/27_OCI_Operations_Overlay_OCI.docx
CCoE_Build_Kit_v1_300Courts/90_OPERATIONS/28_SOP_Catalog_Index.docx
CCoE_Build_Kit_v1_300Courts/90_OPERATIONS/29_Template_Runbook.docx
CCoE_Build_Kit_v1_300Courts/90_OPERATIONS/30_Template_Playbook_Scenario_Driven_.docx
CCoE_Build_Kit_v1_300Courts/90_OPERATIONS/31_Template_Shift_Handover.docx
CCoE_Build_Kit_v1_300Courts/90_OPERATIONS/32_Template_Dashboard_Standard.docx
CCoE_Build_Kit_v1_300Courts/90_OPERATIONS/33_Template_Pager_On_Call_Roster.docx
CCoE_Build_Kit_v1_300Courts/90_OPERATIONS/34_Continuous_Monitoring_ConMon_Schedule_Exports.docx
CCoE_Build_Kit_v1_300Courts/90_OPERATIONS/35_Scanning_Operations_CSPM_CWPP_Vuln.docx
CCoE_Build_Kit_v1_300Courts/90_OPERATIONS/36_Asset_Inventory_Reconciliation_Ops_.docx
CCoE_Build_Kit_v1_300Courts/90_OPERATIONS/99_Index_of_Documents.docx
CCoE_Build_Kit_v1_300Courts/90_OPERATIONS/ANNEX_User_Uploaded/
CCoE_Build_Kit_v1_300Courts/90_OPERATIONS/ANNEX_User_Uploaded/01_SRE_Playbook.docx
CCoE_Build_Kit_v1_300Courts/90_OPERATIONS/ANNEX_User_Uploaded/02_Runbooks_Index.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/00_Cover_Sheet.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/01_Terminology_and_Acronyms.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/02_Assurance_Vision_Principles.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/03_Assurance_Operating_Model_Independence_Charter.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/04_Assessment_Scope_Methodology.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/05_Control_Mapping_Traceability_Matrix.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/06_Security_Assessment_Plan_SAP_Template.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/07_Security_Assessment_Report_SAR_Template.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/08_POA_M_Management_Standard.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/09_Readiness_Assessment_Guide_Pre_ATO_.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/10_Continuous_Monitoring_ConMon_Assessment_Playbook.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/11_Vulnerability_Management_Scanning_Assurance.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/12_Penetration_Testing_Rules_of_Engagement_Method.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/13_Privacy_Assessment_PIA_DPIA_Assurance.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/14_Supply_Chain_Risk_SBOM_Assurance.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/15_Configuration_Management_Assurance_Baselines_CMDB_.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/16_Change_Control_Assurance_ITSM_Interface_.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/17_Incident_Response_Forensics_Assurance.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/18_Backup_DR_BCP_Testing_Assurance.docx

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Page 109 of 117

CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/19_Data_Protection_Encryption_Assurance.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/20_Access_Control_Identity_Assurance.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/21_Logging_Monitoring_SIEM_Assurance.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/22_Zero_Trust_Controls_Assurance.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/23_AI_Systems_Assurance_Addendum.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/24_Data_Platform_Assurance_Addendum.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/25_FinOps_Control_Assurance_Addendum.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/26_ITSM_CMP_Assurance_Addendum.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/27_Operations_Assurance_Addendum.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/28_Inheritance_Verification_Playbook_Landing_Zones_.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/29_Assessor_Evidence_Request_Templates.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/30_Audit_Timeline_Communication_Plan.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/31_Sampling_Plan_Populations.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/32_Test_Procedures_Library_Index.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/33_Findings_Classification_Severity_Matrix.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/34_Remediation_Verification_Closure_Procedures.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/35_Executive_Brief_Template_Assessment_Exit_.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/36_Artifact_Naming_Versioning_Standard.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/37_Assessor_Access_Model_Rules.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/38_Evidence_Index_Storage_Locations_Assurance.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/39_AWS_Assurance_Inheritance_Checks_AWS_Landing_Zone.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/40_Azure_Assurance_Inheritance_Checks_Azure_Landing_Zone.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/41_GCP_Assurance_Inheritance_Checks_GCP_Landing_Zone.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/42_OCI_Assurance_Inheritance_Checks_OCI_Landing_Zone.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/43_ATO_Bridge_Statement_Template.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/44_Implementation_Statement_Template_per_Control_.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/45_Assessor_Checklist_Control_Family.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/99_Index_of_Documents.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/ANNEX_User_Uploaded/
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/ANNEX_User_Uploaded/01_Continuous_Monitoring.docx
CCoE_Build_Kit_v1_300Courts/95_ASSURANCE/ANNEX_User_Uploaded/02_Assessment_Templates.docx
CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/
CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/00_Cover_Sheet.docx
CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/01_Terminology_and_Acronyms.docx
CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/02_Training_Enablement_Strategy.docx
CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/03_Audience_Role_Definitions.docx
CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/04_Role_Based_Learning_Paths.docx
CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/05_Curriculum_Matrix_by_Role_Level.docx
CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/06_Certification_Map_by_Cloud_Role.docx
CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/07_Court_Onboarding_Ramp_Plan.docx
CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/08_Train_the_Trainer_T3_Program.docx

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Page 110 of 117

CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/09_LMS_Content_Standards_SCORM_xAPI_.docx
CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/10_Accessibility_Section_508_Compliance.docx
CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/11_Lab_Governance_Safety_No_Data_Exfil_IL_like_constraints_.docx
CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/12_Lab_Environment_Provisioning_Standard_Per_Cloud.docx
CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/13_Labs_Migration_Factory_Fundamentals.docx
CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/14_Labs_Landing_Zones_Identity.docx
CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/15_Labs_Security_Zero_Trust.docx
CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/16_Labs_Data_Platform.docx
CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/17_Labs_DevSecOps_CI_CD.docx
CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/18_Labs_Operations_ConMon.docx
CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/19_Labs_FinOps.docx
CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/20_Simulation_Exercises_Incident_DR_Audit_ATO.docx
CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/21_Knowledge_Checks_Assessments_Template.docx
CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/22_Coaching_Office_Hours_SOP.docx
CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/23_Communications_Change_Management_OCM_.docx
CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/24_Adoption_Metrics_KPIs.docx
CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/25_Instructor_Guide_Template.docx
CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/26_Lesson_Plan_Template.docx
CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/27_Participant_Guide_Template.docx
CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/28_Capstone_Project_Guide.docx
CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/29_ATO_RMF_Training_Module_Outline.docx
CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/30_Privacy_Ethics_incl._AI_Module_Outline.docx
CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/31_AWS_AWS_Training_Overlay_Path_Modules.docx
CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/32_AWS_AWS_Lab_Catalog_Shortlist.docx
CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/33_Azure_Azure_Training_Overlay_Path_Modules.docx
CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/34_Azure_Azure_Lab_Catalog_Shortlist.docx
CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/35_GCP_GCP_Training_Overlay_Path_Modules.docx
CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/36_GCP_GCP_Lab_Catalog_Shortlist.docx
CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/37_OCI_OCI_Training_Overlay_Path_Modules.docx
CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/38_OCI_OCI_Lab_Catalog_Shortlist.docx
CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/39_Evidence_Index_&_Storage_Locations_Training_Enablement.docx
CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/99_Index_of_Documents.docx
CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/ANNEX_User_Uploaded/
CCoE_Build_Kit_v1_300Courts/96_TRAINING_ENABLEMENT/ANNEX_User_Uploaded/01_Role_Based_Training.docx

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Page 111 of 117

CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/00_Cover_Sheet.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/01_Terminology_and_Acronyms.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/02_Change_Management_Policy.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/03_Change_Types_Criteria_Standard_Normal_Emergency_.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/04_Risk_Assessment_Scoring_Model.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/05_Impact_Analysis_Dependency_Mapping.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/06_RFC_Workflow_Digital_Approvals.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/07_CAB_Charter.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/08_ECAB_Procedure_Emergency_Change_.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/09_Change_Schedule_Calendar_Management.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/10_Pre_Implementation_Validation_Testing_Standard.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/11_Backout_Rollback_Strategy_Standard.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/12_Post_Implementation_Review_PIR_Policy.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/13_Evidence_Bundle_Audit_Trail_Requirements.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/14_Integration_with_CI_CD_DevSecOps_Gates.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/15_IaC_Baseline_Control_Drift_Configuration_.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/16_SBOM_Supply_Chain_Change_Control.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/17_Secrets_Keys_Certificates_Change_Procedures.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/18_Database_Change_Management_Standard.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/19_Data_Migration_Cutover_Change_Control.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/20_Platform_Infra_Change_Procedures_Network_DNS_Firewall_.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/21_Security_Change_Control_IAM_KMS_Policies_.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/22_Access_Change_Requests_Privileged_JIT_JEA_.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/23_Emergency_Hotfix_Procedure.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/24_Freeze_Exception_Workflow.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/25_Change_Communication_Plan_Stakeholder_Matrix.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/26_Change_Metrics_KPIs.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/27_FedRAMP_NIST_800_53_Mapping_Change_Management.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/28_ATO_Evidence_Map_Change_Control.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/29_AWS_Change_Overlay_Systems_Manager_Pipelines.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/30_Azure_Change_Overlay_Update_Manager_Change_Analysis.docx

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Page 112 of 117

CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/31_GCP_Change_Overlay_Cloud_Deploy_Audit_Logs.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/32_OCI_Change_Overlay_Resource_Manager_Events.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/33_Template_Request_for_Change_RFC_.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/34_Template_Change_Plan_Backout.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/35_Template_Testing_Results_Signoffs.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/36_Template_Approval_Sheet_Digital_Signatures_.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/37_Template_Post_Implementation_Review_PIR_.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/38_Template_Freeze_Exception_Request.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/39_Template_Change_Communications.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/40_Runbook_Standard_Change_Execution.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/41_Runbook_Normal_Change_Execution.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/42_Runbook_Emergency_Change_Execution_ECAB_.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/43_Runbook_Change_Calendar_Operations.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/44_Runbook_Evidence_Export_for_ATO_Assessors.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/99_Index_of_Documents.docx
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/ANNEX_User_Uploaded/
CCoE_Build_Kit_v1_300Courts/97_CHANGE_MANAGEMENT/ANNEX_User_Uploaded/01_CCB_Charter.docx
CCoE_Build_Kit_v1_300Courts/98_REFERENCES/
CCoE_Build_Kit_v1_300Courts/98_REFERENCES/00_Cover_Sheet.docx
CCoE_Build_Kit_v1_300Courts/98_REFERENCES/01_Terminology_and_Acronyms.docx
CCoE_Build_Kit_v1_300Courts/98_REFERENCES/02_Master_Bibliography_Guidance.docx
CCoE_Build_Kit_v1_300Courts/98_REFERENCES/03_Citation_Style_Federal_Tech_Programs.docx
CCoE_Build_Kit_v1_300Courts/98_REFERENCES/04_Standards_Frameworks_Index.docx
CCoE_Build_Kit_v1_300Courts/98_REFERENCES/05_NIST_SP_800_53_Rev.5_Control_Families_Summary_.docx
CCoE_Build_Kit_v1_300Courts/98_REFERENCES/06_NIST_SP_800_37_RMF_Summary.docx
CCoE_Build_Kit_v1_300Courts/98_REFERENCES/07_FedRAMP_Baselines_Moderate_High_Overview_.docx
CCoE_Build_Kit_v1_300Courts/98_REFERENCES/08_DoD_Cloud_Computing_SRG_IL2_IL4_IL5_IL6_Overview_Mapping_Notes_.docx
CCoE_Build_Kit_v1_300Courts/98_REFERENCES/09_CJIS_Security_Policy_Summary.docx
CCoE_Build_Kit_v1_300Courts/98_REFERENCES/10_CISA_Binding_Operational_Directives_Index.docx
CCoE_Build_Kit_v1_300Courts/98_REFERENCES/11_FIPS_140_3_Cryptographic_Validation_Summary_.docx
CCoE_Build_Kit_v1_300Courts/98_REFERENCES/12_Zero_Trust_References_NIST_SP_800_207_CISA_ZTMM.docx
CCoE_Build_Kit_v1_300Courts/98_REFERENCES/13_CIS_Benchmarks_Index.docx
CCoE_Build_Kit_v1_300Courts/98_REFERENCES/14_STIGs_Common_Platforms_Index.docx
CCoE_Build_Kit_v1_300Courts/98_REFERENCES/15_Privacy_References_Privacy_Act_OMB_NIST.docx
CCoE_Build_Kit_v1_300Courts/98_REFERENCES/16_CUI_Marking_Handling_Quick_Guide.docx
CCoE_Build_Kit_v1_300Courts/98_REFERENCES/17_Section_508_Accessibility_Standards_Summary_.docx

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Page 113 of 117

CCoE_Build_Kit_v1_300Courts/98_REFERENCES/18_Software_Supply_Chain_NIST_SSDF_SP_800_218_SBOM.docx
CCoE_Build_Kit_v1_300Courts/98_REFERENCES/19_Security_Testing_Scanning_Reference_Index_SCAP_Nessus_OpenSCAP_.docx
CCoE_Build_Kit_v1_300Courts/98_REFERENCES/20_E_Discovery_Records_Management_NARA.docx
CCoE_Build_Kit_v1_300Courts/98_REFERENCES/21_Reference_Matrix_Control_Evidence_Source.docx
CCoE_Build_Kit_v1_300Courts/98_REFERENCES/22_Citation_Register_Master_Template.docx
CCoE_Build_Kit_v1_300Courts/98_REFERENCES/23_Source_Reliability_Versioning_Policy.docx
CCoE_Build_Kit_v1_300Courts/98_REFERENCES/24_AWS_AWS_Official_References_Index.docx
CCoE_Build_Kit_v1_300Courts/98_REFERENCES/25_Azure_Azure_Official_References_Index.docx
CCoE_Build_Kit_v1_300Courts/98_REFERENCES/26_GCP_GCP_Official_References_Index.docx
CCoE_Build_Kit_v1_300Courts/98_REFERENCES/27_OCI_OCI_Official_References_Index.docx
CCoE_Build_Kit_v1_300Courts/98_REFERENCES/28_Identity_Standards_FIPS_201_3_PIV_OIDC_SAML.docx
CCoE_Build_Kit_v1_300Courts/98_REFERENCES/29_Data_Standards_NIEM_CJIS_Domain_Models_FIPS.docx
CCoE_Build_Kit_v1_300Courts/98_REFERENCES/30_Encryption_Key_Management_SP_800_57_130_175_38.docx
CCoE_Build_Kit_v1_300Courts/98_REFERENCES/31_Incident_Response_NIST_SP_800_61r2.docx
CCoE_Build_Kit_v1_300Courts/98_REFERENCES/32_BCDR_NIST_SP_800_34_Rev.1.docx
CCoE_Build_Kit_v1_300Courts/98_REFERENCES/33_Cloud_SLA_Contracting_FAR_GSA_Agency_Refs.docx
CCoE_Build_Kit_v1_300Courts/98_REFERENCES/34_Safe_Harbor_Common_URLs_Persistent_Links_Template_.docx
CCoE_Build_Kit_v1_300Courts/98_REFERENCES/35_Evidence_Bookmarks_Storage_Paths_Access.docx
CCoE_Build_Kit_v1_300Courts/98_REFERENCES/99_Index_of_Documents.docx
CCoE_Build_Kit_v1_300Courts/98_REFERENCES/ANNEX_User_Uploaded/
CCoE_Build_Kit_v1_300Courts/98_REFERENCES/ANNEX_User_Uploaded/01_Standards.docx
CCoE_Build_Kit_v1_300Courts/999_ANNEXS/
CCoE_Build_Kit_v1_300Courts/999_ANNEXS/00_Cover_Sheet.docx
CCoE_Build_Kit_v1_300Courts/999_ANNEXS/01_Terminology_and_Acronyms.docx
CCoE_Build_Kit_v1_300Courts/999_ANNEXS/02_Annexes_Overview_Instructions.docx
CCoE_Build_Kit_v1_300Courts/999_ANNEXS/03_Document_Control_Log.docx
CCoE_Build_Kit_v1_300Courts/999_ANNEXS/04_Version_History_Log.docx
CCoE_Build_Kit_v1_300Courts/999_ANNEXS/05_Distribution_List.docx
CCoE_Build_Kit_v1_300Courts/999_ANNEXS/06_Program_Contacts_Roster.docx
CCoE_Build_Kit_v1_300Courts/999_ANNEXS/07_Meeting_Minutes_Template.docx
CCoE_Build_Kit_v1_300Courts/999_ANNEXS/08_Decisions_Log_D-Register_.docx
CCoE_Build_Kit_v1_300Courts/999_ANNEXS/09_Risks_Issues_Actions_RAID_.docx
CCoE_Build_Kit_v1_300Courts/999_ANNEXS/10_Change_Log_Program.docx
CCoE_Build_Kit_v1_300Courts/999_ANNEXS/11_Court_Roster_Cloud_Selection_Register.docx
CCoE_Build_Kit_v1_300Courts/999_ANNEXS/12_Court_Onboarding_Checklist_Template.docx
CCoE_Build_Kit_v1_300Courts/999_ANNEXS/13_Data_Classification_Register_Template.docx
CCoE_Build_Kit_v1_300Courts/999_ANNEXS/14_Data_Tagging_Taxonomy.docx
CCoE_Build_Kit_v1_300Courts/999_ANNEXS/15_Asset_Inventory_Register_Template.docx
CCoE_Build_Kit_v1_300Courts/999_ANNEXS/16_Vendor_Contract_Register.docx
CCoE_Build_Kit_v1_300Courts/999_ANNEXS/17_Interconnections_MOUs_Register.docx
CCoE_Build_Kit_v1_300Courts/999_ANNEXS/18_Training_Attendance_Completion_Log.docx

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Page 114 of 117

CCoE_Build_Kit_v1_300Courts/999_ANNEXS/19_Access_Attestation_Log.docx
CCoE_Build_Kit_v1_300Courts/999_ANNEXS/20_Evidence_Export_Catalog_Template.docx
CCoE_Build_Kit_v1_300Courts/999_ANNEXS/21_Control_Inheritance_Evidence_Index.docx
CCoE_Build_Kit_v1_300Courts/999_ANNEXS/22_Court_Migration_Wave_Pack_Index.docx
CCoE_Build_Kit_v1_300Courts/999_ANNEXS/23_Court_Binder_Annex_Shell.docx
CCoE_Build_Kit_v1_300Courts/999_ANNEXS/24_Architecture_Diagrams_Register.docx
CCoE_Build_Kit_v1_300Courts/999_ANNEXS/25_Figures_List_Captions_Template.docx
CCoE_Build_Kit_v1_300Courts/999_ANNEXS/26_Baseline_Standards_Register.docx
CCoE_Build_Kit_v1_300Courts/999_ANNEXS/27_References_Citation_Shortlist_Annex_.docx
CCoE_Build_Kit_v1_300Courts/999_ANNEXS/28_Repository_Share_Paths_Index.docx
CCoE_Build_Kit_v1_300Courts/999_ANNEXS/29_ATO_Evidence_Attachments_Index_Annex_.docx
CCoE_Build_Kit_v1_300Courts/999_ANNEXS/30_CJIS_Legal_Constraints_Register.docx
CCoE_Build_Kit_v1_300Courts/999_ANNEXS/31_Privacy_Artifacts_Register_PTA_PIA_.docx
CCoE_Build_Kit_v1_300Courts/999_ANNEXS/32_Template_Court_Migration_Annex_Checklist.docx
CCoE_Build_Kit_v1_300Courts/999_ANNEXS/33_Template_Evidence_Bundle_Cover_Sheet.docx
CCoE_Build_Kit_v1_300Courts/999_ANNEXS/99_Index_of_Documents.docx
CCoE_Build_Kit_v1_300Courts/999_ANNEXS/ZZ_Stamping_Instructions.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/
CCoE_Build_Kit_v1_300Courts/99_ATOS/00_COE/
CCoE_Build_Kit_v1_300Courts/99_ATOS/00_COE/ATO_00_Overview.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/00_COE/ATO_01_FIPS199.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/00_COE/ATO_02_SSP_TOC.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/00_COE/ATO_03_Control_Implementation_Summary_Template.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/00_COE/ATO_04_Customer_Responsibility_Matrix_Template.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/00_COE/ATO_05_POAM_Template.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/00_COE/ATO_06_Continuous_Monitoring_Strategy.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/00_COE/ATO_07_Incident_Response_Playbooks_Index.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/00_COE/ATO_08_SAP_Template.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/00_COE/ATO_09_SAR_Template.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/00_COE/ATO_10_Authorization_Boundary.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/00_COE/ATO_11_Interconnections_ISA_Skeleton.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/00_COE/ATO_12_Privacy_Threshold_Analysis_Template.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/00_COE/ATO_13_Personnel_Screening_and_Training.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/00_COE/ATO_14_Configuration_Management_Plan.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/00_COE/ATO_15_Contingency_Plan.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/00_COE/ReadMe.md
CCoE_Build_Kit_v1_300Courts/99_ATOS/00_Cover_Sheet.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/01_Terminology_and_Acronyms.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/02_ATO_Program_Guide_Process.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/03_FIPS_199_Categorization_E_Authentication_Risk_Assessment.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/04_System_Boundary_Data_Flow_Register.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/05_Roles_Responsibilities_ATO.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/06_Control_Inheritance_Strategy_Landing_Zones_CSPs_.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/07_System_Security_Plan_SSP_Template.docx

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

CCoE_Build_Kit_v1_300Courts/99_ATOS/08_Control_Implementation_Statements_Index.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/09_Common_Control_Workbook_Template.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/10_Attachments_Register_SSP_A_Z_.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/11_Security_Assessment_Plan_SAP_Template_3PAO_.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/12_Rules_of_Engagement_ROE_for_Testing.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/13_Security_Assessment_Report_SAR_Template.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/14_POA_M_Template.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/15_Continuous_Monitoring_Strategy.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/16_ConMon_Monthly_Quarterly_Package_Index.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/17_Vulnerability_Scanning_Requirements_Authenticated_.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/18_Penetration_Test_Plan_Report_Templates.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/19_Contingency_Plan_CP_Test_Results_ATO_View.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/20_Incident_Response_Plan_IRP_Playbooks_ATO_View.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/21_Configuration_Management_CM_ATO_Interface.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/22_Privacy_PTA_PIA_Templates.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/23_Interconnection_Security_Agreements_ISA_Template.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/24_Encryption_Key_Management_Summary.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/25_Ports_Protocols_Services_PPS_Register.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/26_Hardware_Software_Inventory_Baseline.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/27_Scan_Credentials_Access_Attestation_SOP.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/28_Deviation_Requests_Risk_Acceptance_Template.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/29_POA_M_Review_Board_PRB_Charter.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/30_ATO_Decision_Package_Assembly_Checklist.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/31_ATO_Letter_Draft_Template.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/32_Reciprocity_Reuse_Memo_Template.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/33_Court_Execution_Binder_ATO_Section_Index.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/34_Evidence_Index_Storage_Locations_ATO.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/35_FedRAMP_Baseline_Matrix_Moderate_High.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/36_Control_Crosswalk_FedRAMP_CJIS_DoD_SRG.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/37_Quarterly_Assessment_Addendum_SAR_Lite_.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/38_Annual_Assessment_Plan.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/39_Assessor_Access_SOP_ATO_Repository.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/40_Audit_Trail_Export_Process_ATO.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/41_Risk_Register_Template.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/42_AWS_ATO_Overlay_AWS_GovCloud_Commercial_Inheritance_Workbook_.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/43_Azure_ATO_Overlay_Azure_Government_Commercial_Inheritance_Workbook_.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/44_GCP_ATO_Overlay_GCP_Assured_Workloads_Inheritance_Workbook_.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/45_OCI_ATO_Overlay_OCI_Inheritance_Workbook_.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/99_Index_of_Documents.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/ANNEX_User_Uploaded/
CCoE_Build_Kit_v1_300Courts/99_ATOS/ANNEX_User_Uploaded/ATO_00_Overview.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/ANNEX_User_Uploaded/ATO_01_FIPS199.docx

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

CCoE_Build_Kit_v1_300Courts/99_ATOS/ANNEX_User_Uploaded/ATO_02_SSP_TOC.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/ANNEX_User_Uploaded/ATO_03_Control_Implementation_Summary_Template.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/ANNEX_User_Uploaded/ATO_04_Customer_Responsibility_Matrix_Template.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/ANNEX_User_Uploaded/ATO_05_POAM_Template.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/ANNEX_User_Uploaded/ATO_06_Continuous_Monitoring_Strategy.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/ANNEX_User_Uploaded/ATO_07_Incident_Response_Playbooks_Index.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/ANNEX_User_Uploaded/ATO_08_SAP_Template.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/ANNEX_User_Uploaded/ATO_09_SAR_Template.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/ANNEX_User_Uploaded/ATO_10_Authorization_Boundary.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/ANNEX_User_Uploaded/ATO_11_Interconnections_ISA_Skeleton.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/ANNEX_User_Uploaded/ATO_12_Privacy_Threshold_Analysis_Template.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/ANNEX_User_Uploaded/ATO_13_Personnel_Screening_and_Training.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/ANNEX_User_Uploaded/ATO_14_Configuration_Management_Plan.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/ANNEX_User_Uploaded/ATO_15_Contingency_Plan.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/ANNEX_User_Uploaded/ReadMe.docx
CCoE_Build_Kit_v1_300Courts/99_ATOS/__tmp.docx

All information contained adheres to DoD IL4/IL5/IL6, FedRAMP High, and NIST SP 800-53 Rev. 5 controls.

Page 117 of 117