www.verdantialaw.com

LEGAL MODERNIZATION PLAYBOOK

Foreword

THIS PLAYBOOK WAS DEVELOPED TO ADDRESS THE WIDENING GAP BETWEEN THE OPERATIONAL DEMANDS PLACED ON LEGAL INSTITUTIONS AND THE MATURITY OF THEIR SUPPORTING IT SYSTEMS. AMID ESCALATING CYBERSECURITY THREATS, REGULATORY SCRUTINY, AND DIGITAL DISRUPTION, LEGAL FIRMS MUST MOVE BEYOND REACTIVE PATCHWORK SOLUTIONS AND EMBRACE STRUCTURED, SECURE MODERNIZATION.

ROOTED IN BOTH PRACTICE AND POLICY, THIS PLAYBOOK DRAWS ON U.S. FEDERAL MODERNIZATION MANDATES INCLUDING EXECUTIVE ORDER 14028, THE NATIONAL CYBERSECURITY STRATEGY, AND OMB M-22-09. IT ALIGNS LEGAL SECTOR IT TRANSFORMATION WITH ZERO TRUST ARCHITECTURE, INSTITUTIONAL RESILIENCE PRINCIPLES, AND MODERN GOVERNANCE FRAMEWORKS

.

THE GUIDANCE HEREIN IS GROUNDED IN REAL-WORLD IMPLEMENTATION EXPERIENCE ACROSS LAW FIRMS, GOVERNMENT PROGRAMS, AND REGULATED SECTORS. IT OFFERS NOT JUST STRATEGY, BUT EXECUTION: A FRAMEWORK OF TOOLS, MODELS, AND BEST PRACTICES TO MOVE FROM ASSESSMENT TO MATURITY. WHETHER YOU ARE LAUNCHING YOUR FIRST DIGITAL AUDIT OR SCALING AN ENTERPRISE TRANSFORMATION, THIS RESOURCE IS BUILT TO GUIDE YOUR JOURNEY

.

WELCOME TO THE LEGAL MODERNIZATION PLAYBOOK. THIS INTERACTIVE WEB-BASED RESOURCE IS DESIGNED TO HELP LEGAL AND COMPLIANCE-DRIVEN INSTITUTIONS MODERNIZE THEIR LEGACY IT SYSTEMS WITH CONFIDENCE, SECURITY, AND STRATEGIC ALIGNMENT TO FEDERAL PRIORITIES. IT INCLUDES DETAILED DOMAIN GUIDANCE, ASSESSMENT TOOLS, IMPLEMENTATION ROADMAPS, AND GOVERNANCE FRAMEWORKS TO ACCELERATE SECURE DIGITAL TRANSFORMATION ACROSS LEGAL INSTITUTIONS.

TABLE OF CONTENTS

Executive Summary

The U.S. legal and regulatory sectors face growing pressure to modernize legacy systems. Security risks, client expectations, and federal policies such as Executive Order 14028 and OMB M-22-09 have made modernization an urgent strategic priority. This playbook helps legal CIOs, IT Directors, and operational leaders benchmark their maturity, reduce risks, and implement sustainable improvements.

Modernization is not only a technical exercise it is a transformation of people, process, and platforms.

This playbook offers:

- A self-assessment tool across eight legal IT maturity domains
- Maturity models with 1–5 scoring scales and recommendations
- U.S. federal policy alignment (EO 14028, OMB M-22-09, NIST)
- Ready-to-use templates, workflows, and transformation blueprints

Audience

- Legal CIOs and IT Directors
- Managing Partners and Legal Operations Leaders
- Compliance and Risk Officers
- Law firm technology advisors and consultants

How to use Playbook

1. **Assess Your Maturity**: Begin with a diagnostic tool covering eight domains.
2. **Analyze Results**: Understand your current state with maturity banding.
3. **Target Improvements**: Use domain-specific guidance to prioritize efforts.
4. **Implement Change**: Apply the roadmap and governance model.
5. **Track Progress**: Reassess maturity periodically and report outcomes

Domains of Legal Modernisation

Each domain includes:

- 5 maturity subdomains (People, Process, Tooling, Data, Continual Improvement)
- 5-level scoring model (Initial to Optimized)
- Maturity descriptors
- Federal mapping
- Recommendations
- Tools and templates

CyberSecurity

Overview

Cybersecurity is foundational to trust and regulatory compliance in the legal sector. Legal institutions manage sensitive client data, protected health information (PHI), and privileged communications, making them prime targets for cyberattacks. This domain helps organizations secure their systems by adopting Zero Trust principles and aligning with NIST and federal cybersecurity mandates

Maturity Sub Domains

- People & Organization
- Process
- Tooling
- Data
- Continual Improvement

Maturity Model

Score	Maturity Level	Description
1.0 to 1.9	Initial	Security practices are informal, ad hoc, or nonexistent. No dedicated ownership.
2.0 to 2.9	Developing	Basic controls exist but are inconsistently applied. Partial awareness of threats.
3.0 to 3.9	Established	Roles, policies, and tooling are in place. Security is documented and reviewed.
4.0 to 4.9	Managed	Threat intelligence, advanced monitoring, and governance practices are embedded.
5	Optimised	Zero Trust architecture is fully implemented. Security is automated, proactive, and benchmarked.

Federal Aligment

- Executive Order 14028 – Mandates endpoint detection, logging, and coordinated incident response.
- OMB M-22-09 – Requires Zero Trust architecture adoption across five pillars.
- National Cybersecurity Strategy (2023) – Prioritizes risk reduction, sector resilience, and vendor accountability.

Typical Recommendations

- **Initial**: Appoint a security lead. Document a minimum incident response plan. Conduct basic phishing awareness.
- **Developing**: Deploy MFA, endpoint protection, and encryption. Establish access management policies.
- **Established**: Implement vulnerability scanning, centralized logging, and SIEM tools. Begin Zero Trust design.
- **Managed**: Formalize threat detection playbooks. Integrate security telemetry. Automate compliance checks.
- **Optimized**: Conduct red teaming. Participate in legal threat-sharing programs. Leverage AI-enhanced defense.

Sample KPIs

- % endpoints with updated AV/MFA
- % of detected vs. resolved incidents per quarter
- % of systems covered by Zero Trust controls
- Time-to-remediate (TTR) vs. industry benchmark

Tools & Templates

- Incident Response Plan Template
- Cybersecurity Policy Framework (aligned to NIST 800-53)
- Zero Trust Adoption Checklist
- Legal Sector Security Tool Evaluation Matrix Secures critical systems and aligns with Zero Trust principles. Addresses identity, endpoint, network, and threat management

Risk & Compliance

Overview

In the legal sector, risk and compliance management ensures institutions meet regulatory expectations, protect client confidentiality, and avoid reputational and financial penalties. This domain focuses on building resilient, transparent processes that align with internal policy controls and external standards such as ABA Model Rules, SOC 2, and ISO 27001.

Maturity Sub Domains

- People & Organization
- Process
- Tooling
- Data
- Continual Improvement

Maturity Model

Score	Maturity Level	Description
1.0 to 1.9	Initial	Responsibilities are unclear; few formal policies or controls in place.
2.0 to 2.9	Developing	Some risk and compliance practices exist but are reactive or fragmented.
3.0 to 3.9	Established	Defined governance structure; regular audits and reviews occur.
4.0 to 4.9	Managed	Risks are quantified, prioritized, and tracked across departments.
5	Optimised	Integrated compliance and risk platforms with predictive insights.

Risk & Compliance

Federal Aligment

- Executive Order 14028 – Promotes robust compliance governance and supply chain risk transparency.
- SOC 2 & ISO 27001 – Drive data protection and auditability expectations in client/vendor relationships.
- DOJ Evaluation of Corporate Compliance Programs – Encourages institutionalized risk accountability.

Typical Recommendations

- **Initial:** Assign compliance responsibility. Begin mapping policies to controls. Educate staff.
- **Developing:** Document compliance processes. Initiate risk log. Begin internal audit planning.
- **Established:** Implement GRC tooling. Align controls to SOC 2 or ISO 27001. Track regulatory change.
- **Managed:** Conduct periodic internal and external audits. Visualize key risks. Link mitigation plans to action owners.
- **Optimized:** Automate compliance checks. Establish policy lifecycle workflows. Use analytics for forecasting.

Sample KPIs

- % policies mapped to control frameworks
- of unresolved risks past SLA
- % of departments completing quarterly compliance reviews
- Compliance audit pass rate

Tools & Templates

- Compliance Obligation Register Template
- Risk Register with Likelihood × Impact Matrix
- Internal Audit Planning Template
- Policy Review Schedule & Escalation Workflow Enables traceable, auditable compliance with internal policies and external regulations[10] (ABA, SOC2, ISO 27001).

Incident & Problem Mngt

Overview

Incident and problem management ensures service continuity, preserves client confidence, and protects the integrity of legal operations. This domain enables firms to reduce downtime, respond effectively to technology disruptions, and learn from root cause analysis to prevent recurrence.

Maturity Sub Domains

- People & Organization
- Process
- Tooling
- Data
- Continual Improvement

Maturity Model

Score	Maturity Level	Description
1.0 to 1.9	Initial	No formal process or documentation. Incident handling is reactive and inconsistent.
2.0 to 2.9	Developing	Some structure exists, but response and communication remain inconsistent.
3.0 to 3.9	Established	Defined roles and processes for triage, resolution, and root cause analysis.
4.0 to 4.9	Managed	Integrated tooling, performance SLAs, and trend analysis in place.
5	Optimised	Predictive analytics and proactive monitoring used to minimize impact.

Incident & Problem Mngt

Federal Aligment

- Executive Order 14028 – Requires endpoint detection, central logging, and incident coordination.
- OMB M-22-09 – Emphasizes visibility and incident response integration within Zero Trust.
- NIST CSF (Respond/Recover Functions) – Provides process maturity guidelines for security events.

Typical Recommendations

- **Initial:** Assign incident response roles. Create basic incident response workflows.
- **Developing:** Define severity levels, communication procedures, and tracking methods.
- **Established:** Formalise root cause analysis, post-mortems, and escalation rules.
- **Managed:** Implement SLA tracking, trend dashboards, and automation for ticket routing.
- **Optimized:** Use predictive analytics and ML-based triage. Engage in continuous service improvement.

Sample KPIs

- Mean Time to Resolution (MTTR)
- % of incidents resolved within SLA
- of recurring incidents linked to root cause
- User satisfaction with incident handling

Tools & Templates

- Incident Escalation Matrix
- Post-Incident Review Template
- Problem Management Register
- Incident Severity Classification Guide Creates formal, repeatable response structures to minimize service disruption and prevent recurrence.

Service Continuity & Resilience

Overview

Legal services depend on continuous access to critical systems, especially during litigation, regulatory events, or service-level commitments. This domain ensures that organizations can respond to and recover from disruptions whether natural disasters, cyberattacks, or infrastructure failures, with minimal impact on clients and operations.

Maturity Sub Domains

- People & Organization
- Process
- Tooling
- Data
- Continual Improvement

Maturity Model

Score	Maturity Level	Description
1.0 to 1.9	Initial	No formal continuity or recovery planning. Highly reactive and undocumented.
2.0 to 2.9	Developing	Some business continuity plans exist but are outdated, siloed, or untested.
3.0 to 3.9	Established	Documented and tested continuity plans. Core systems mapped and protected.
4.0 to 4.9	Managed	Continuity integrated into IT operations, with RTOs/RPOs defined and resourced.
5	Optimised	Continuous resilience testing, real-time failover, and board-level reporting.

Service Continuity & Resilience

Federal Aligment

- National Cybersecurity Strategy (2023) – Emphasises continuity and risk reduction.
- FEMA and NIST Guidelines – Endorse continuity planning as a critical risk mitigation step.
- ABA Formal Opinion 477R – Encourages operational safeguards for client data availability.

Typical Recommendations

- **Initial:** Assign continuity roles. Inventory business critical applications and services.
- **Developing:** Draft recovery procedures. Establish backup protocols. Conduct tabletop exercises.
- **Established:** Define and test Recovery Time (RTO) and Recovery Point Objectives (RPO).
- **Managed:** Integrate continuity into service design. Monitor resilience metrics. Formalize DR roles.
- **Optimized:** Automate failover. Conduct red team/blue team disaster simulations. Align with ISO 22301.

Sample KPIs

- % of critical services covered by a tested continuity plan
- RTO/RPO variance vs. defined targets
- Frequency of DR tests per year
- of continuity incidents without SLA breach

Tools & Templates

- Business Impact Analysis (BIA) Template
- Disaster Recovery Plan Template
- RTO/RPO Calculation Worksheet
- DR Test Scenario Checklist Supports business continuity, disaster recovery, and resilience across litigation-critical systems.

Knowledge & Data Governance

Overview

Legal institutions rely on high quality, well governed information to support litigation, compliance, and business operations. This domain promotes structured control over knowledge and data assets, enabling better collaboration, risk management, and decision making. It supports metadata consistency, document lifecycle management, and institutional knowledge retention.

Maturity Sub Domains

- People & Organization
- Process
- Tooling
- Data
- Continual Improvement

Maturity Model

Score	Maturity Level	Description
1.0 to 1.9	Initial	Knowledge and data are unmanaged, siloed, and inconsistently stored.
2.0 to 2.9	Developing	Basic practices in place; inconsistent metadata and classification standards.
3.0 to 3.9	Established	Documented policies and systems for document and data lifecycle.
4.0 to 4.9	Managed	Active governance processes, metadata standards, and audit trails in use.
5	Optimised	AI-enabled tagging, automated classification, and integrated governance platforms.

Knowledge & Data Governance

Federal Aligment

- OMB M-19-21 – Emphasises transition to fully digital record keeping.
- EO 14028 – Requires traceability of records and secure access to data.
- ABA Model Rules (1.1, 1.6) – Emphasise technological competence and confidentiality.

Typical Recommendations

- **Initial:** Inventory document repositories. Assign ownership of knowledge governance.
- **Developing:** Define metadata standards and retention rules. Consolidate platforms.
- **Established:** Implement DMS workflows. Formalize review, archiving, and versioning.
- **Managed: M**onitor document integrity. Automate classification and de-duplication.
- **Optimized:** Use AI to extract insights. Govern knowledge across the full lifecycle.

Sample KPIs

- % of documents tagged with standardised metadata
- of redundant or obsolete repositories decommissioned
- % adherence to retention and archiving rules
- Accuracy of search and retrieval for key document types

Tools & Templates

- Knowledge Asset Inventory Tracker
- Metadata Governance Checklist
- Document Lifecycle Policy Template
- DMS Audit & Clean Up Workbook

Change & Deployment

Overview

Controlled and well structured change management ensures that technology updates do not disrupt legal operations or jeopardise compliance. This domain evaluates how effectively legal institutions initiate, assess, authorise, implement, and review IT changes.

Maturity Sub Domains

- People & Organization
- Process
- Tooling
- Data
- Continual Improvement

Maturity Model

Score	Maturity Level	Description
1.0 to 1.9	Initial	Changes are unmanaged, undocumented, and often result in incidents.
2.0 to 2.9	Developing	Basic change procedures exist but are inconsistently followed.
3.0 to 3.9	Established	Formal change advisory process with defined change types and impact ratings.
4.0 to 4.9	Managed	Tool supported change management with approval workflows, risk scoring, and rollback plans.
5	Optimised	Fully automated change pipelines, integrated with DevOps, risk engines, and release KPIs.

Change & Deployment

Federal Aligment

- Executive Order 14028 – Emphasises secure software supply chains and validated change controls.
- NIST SP 800-128 – Recommends structured configuration and change control.

Typical Recommendations

- **Initial:** Create a change log. Define who approves technical changes.
- **Developing:** Use change request templates. Identify upstream/downstream dependencies.
- **Established: I**mplement CAB. Assign change roles. Define business impact scoring.
- **Managed:** Automate low risk changes. Standardize rollback testing and documentation.
- **Optimized:** Integrate CI/CD with governance tools. Analyze trends in change success/failure.

Sample KPIs

- % of changes with rollback plan
- % of emergency changes vs. planned changes
- Change failure rate
- CAB approval turnaround time

Tools & Templates

- Change Request Form
- CAB Agenda Template
- Post Implementation Review Template
- Change Risk Scoring Matrix

Infarstructure & Tooling

Overview

Reliable, secure, and scalable infrastructure underpins all legal technology services. Outdated systems introduce cyber risks, performance issues, and compliance gaps. This domain assesses the institution’s ability to manage, modernize, and optimize its infrastructure and tooling stack.

Maturity Sub Domains

- People & Organization
- Process
- Tooling
- Data
- Continual Improvement

Maturity Model

Score	Maturity Level	Description
1.0 to 1.9	Initial	Infrastructure is largely on premise, undocumented, and prone to failure.
2.0 to 2.9	Developing	Partial virtualization and monitoring; inconsistent updates or standards.
3.0 to 3.9	Established	Core systems are virtualized or hybrid; IT asset management and monitoring are in place.
4.0 to 4.9	Managed	Infrastructure is cloud optimised, resilient, and integrated across environments.
5	Optimised	API driven infrastructure with full automation, redundancy, and self-healing capabilities

Infarstructure & Tooling

Federal Aligment

- OMB M-22-09 – Promotes scalable, secure infrastructure with Zero Trust support.
- CISA Zero Trust Maturity Model – Encourages secure, adaptive infrastructure foundations.
- NIST 800-53 Rev. 5 – Recommends consistent system configuration and availability controls.

Typical Recommendations

- **Initial:** Inventory physical and virtual infrastructure. Identify unsupported or high risk assets.
- **Developing:** Standardise patching cycles. Introduce monitoring and backup processes.
- **Established:** Consolidate and virtualise servers. Align toolsets with ITIL or NIST controls.
- **Managed:** Move priority systems to cloud or hybrid. Automate provisioning and scaling.
- **Optimized:** Implement infrastructure as code. Integrate observability tools and SLA metrics.

Sample KPIs

- % of systems compliant with patch management policy
- System uptime (monthly)
- % of workloads hosted in resilient cloud environments
- Mean time to recovery (MTTR) after outage

Tools & Templates

- Infrastructure Audit Template
- Tooling Inventory & Rationalization Matrix
- Cloud Readiness Assessment Checklist
- SLA Monitoring Dashboard Starter Kit

Service Management & Strategy

Overview

Effective service management ensures that IT operations directly support legal business objectives. This domain evaluates how legal institutions define, deliver, and continuously improve IT services in alignment with user expectations and strategic outcomes.

Maturity Sub Domains

- People & Organization
- Process
- Tooling
- Data
- Continual Improvement

Maturity Model

Score	Maturity Level	Description
1.0 to 1.9	Initial	No service catalog or SLAs; reactive support and unclear service ownership.
2.0 to 2.9	Developing	Some defined services and informal SLAs; reporting is inconsistent.
3.0 to 3.9	Established	Standardized service definitions and SLAs; routine service reviews.
4.0 to 4.9	Managed	Service strategy tied to legal priorities; performance monitored and governed.
5	Optimised	Client aligned, value-based service delivery with predictive service modeling.

Service Management & Strategy

Federal Aligment

- ITIL 4 – Establishes a service value system and continual improvement model.
- OMB A-130 – Requires agencies to manage services with performance metrics.
- EO 14028 – Encourages operational transparency and accountability in service delivery.

Typical Recommendations

- **Initial:** Define core legal technology services. Assign service owners. Begin documenting SLAs.
- **Developing:** Create a service catalog. Track basic performance data. Standardize incident categories.
- **Established:** Hold regular service reviews. Develop OLAs and underpinning contracts. Link services to KPIs.
- **Managed:** Align services with business goals. Use dashboards to manage SLAs. Conduct user satisfaction surveys.
- **Optimized:** Use value stream mapping. Integrate service innovation cycles. Benchmark performance externally.

Sample KPIs

- % of services with defined SLAs and OLAs
- Service availability by tier (Gold/Silver/Bronze)
- % of service reviews conducted on schedule
- Net Promoter Score (NPS) for IT services

Tools & Templates

- IT Service Catalog Template
- SLA/OLA Design Workbook
- Service Performance Dashboard Guide
- Balanced Scorecard Template for Legal IT

Federal Aligment

This playbook is designed to work in tandem with your maturity assessment. Once you complete your diagnostic, each score directly maps to a band in the maturity model: Initial, Developing, Established, Managed, or Optimized and unlocks the specific guidance within the relevant section of this playbook. Use the table below to understand what your scores mean and how to act on them:

Score	Maturity Level	Description	Where to Start
1.0 to 1.9	Initial	Practices are largely undocumented or reactive. Major gaps exist in structure, security, or leadership.	Use the foundational checklists and “Initial” maturity recommendations in each domain. Begin with Phase 1 of the roadmap.
2.0 to 2.9	Developing	Some structure exists but practices are inconsistent or siloed. Improvements are underway.	Focus on “Developing” maturity recommendations. Target quick wins in Phase 3 of the roadmap. Prioritize governance setup.
3.0 to 3.9	Established	Core practices are defined and functioning. Risk is managed but optimization is needed.	Follow “Established” and “Managed” sections. Prioritize system integrations and roadmap Phases 3–4.
4.0 to 4.9	Managed	Governance, performance tracking, and policy integration are in place. CI/CD may be emerging.	Scale strategic projects. Strengthen dashboards, SLAs, and proactive controls. Focus on Phase 5 improvements.
5	Optimised	The domain is fully modernized, automated, and delivering measurable value.	Use benchmarking tools. Share practices. Mentor others. Shift toward enterprise-level transformation.

By matching your score to the guidance tier in each domain, you can create a targeted and efficient improvement roadmap. Every domain section in this playbook includes tailored recommendations, KPIs, and downloadable templates that align with these bands.

Strategic Roadmap

Overview

This roadmap outlines a practical, phased approach to legacy IT modernization. Each phase includes specific objectives, recommended actions, and example KPIs to support progress tracking.

Phase 1: Discovery & Assessment

Objectives

Establish baseline understanding of the current IT maturity and risk exposure.

Actions

- Complete the Legal IT Maturity Assessment
- Inventory all critical systems, tools, and data assets
- Identify top 3–5 priority gaps or risks
- Map dependencies across legal, compliance, and business functions

KPIs

- % of systems inventoried
- of risk findings documented
- % completion of maturity assessment across domains

Phase 2: Planning & Governance

Objectives

Formalise leadership, scope, and transformation structure.

Actions

- Establish Modernisation Steering Committee and domain leads
- Define transformation goals, scope, and target maturity scores
- Identify funding, resource needs, and key stakeholders
- Develop high level transformation roadmap

KPIs

- of governance roles assigned
- % of domains with defined scope and KPIs
- Approval of roadmap and budget

Phase 3: Foundations & Quick Wins

Objectives

Build early momentum by resolving critical vulnerabilities and delivering visible value.

Actions

- Implement or formalise incident response and change management processes
- Address known risks (e.g., access gaps, unsupported tools)
- Introduce risk register and service catalog
- Deploy high value improvements (e.g., MFA, backups)

KPIs

- % of quick win actions completed
- of critical risks mitigated
- User feedback on changes implemented

Phase 4: Transformation Projects

Objectives

Deliver major modernization efforts in line with roadmap and policy requirements.

Actions

- Upgrade or replace legacy systems (e.g., DMS, financial tools)
- Migrate services to cloud or hybrid environments
- Pilot and adopt Zero Trust security architecture
- Rationalize and integrate IT tooling

KPIs

- % project milestones completed on time
- of legacy systems decommissioned
- Compliance audit readiness score

Phase 5: Optimization & Scale

Objectives

Institutionalize maturity improvements and create a repeatable improvement cycle.

Actions

- Establish IT performance dashboards and service scorecards
- Benchmark maturity scores year over year
- Integrate continuous improvement into business planning
- Share success metrics with leadership and stakeholders

KPIs

- % of services with real-time performance metrics
- YoY maturity score improvement per domain
- Stakeholder satisfaction ratings

Roadmap Summary

Each phase can be tailored to the firm's size, structure, and risk appetite. Institutions are encouraged to revisit each phase annually to ensure alignment with evolving client expectations and federal policy developments.

Phase 1: Discovery & Assessment

- Run the maturity assessment
- Identify top 3–5 gaps
- Document business-critical services and dependencies

Phase 2: Planning & Governance

- Form a steering group
- Appoint domain leads
- Define scope and KPIs for each initiative

Phase 3: Foundation & Quick Wins

- Secure low effort, high impact improvements
- Introduce incident response and risk registers
- Rationalize duplicative tools

Phase 4: Transformation Projects

- Execute secure modernisation programs (e.g., DMS upgrade, cloud migration)
- Pilot Zero Trust framework
- Retire legacy infrastructure

Phase 5: Optimization & Scale

- Establish service dashboards and KPIs
- Integrate improvements into operational cadence
- Create a maturity improvement cycle

Governance Framework

Structure

- Sponsor: CIO, COO, or Managing Partner
- Steering Committee: Legal Ops, Risk, IT, Business Stakeholders
- Domain Leads: Assigned to each of the 8 domains

Practices

- Monthly governance meetings
- Quarterly risk and roadmap reviews
- KPI reporting and dashboarding
- Stakeholder workshops

Downloadable Templates

- Maturity Assessment Workbook
- Cybersecurity Gap Tracker
- Risk Register & Risk Scoring Matrix
- Change Request & Post-Implementation Review
- DMS Migration Readiness Checklist
- SLA Definition Template
- Continuity Planning Toolkit
- Balanced Scorecard for Legal IT

Start Now

Begin with the Legal IT Maturity Assessment to evaluate your starting point. This playbook is a living tool to support sustained transformation. Use the tools, act on the insights, and lead your institution into a modern, secure, and resilient future.

For additional support, templates, or advisory access, visit www.verdantialaw.com