Mana'o Pili LLC

OPERATIONALIZING 21 CFR PART 11

Designing Audit-Defensible Digital Workflows on the ServiceNow Platform

Keep In Touch With Us

www.manaopili.com

500 Ala Moana Blvd. Suite 7400
Honlolulu, HI 96813

Operationalizing 21 CFR Part 11 in ServiceNow

Rev. January 21, 2026

Electronic Records, Electronic Signatures, and Audit Readiness Using IRM/GRC as Control Systems
Companion White Paper to: Apply FDA Compliance to a ServiceNow Instance (Rev. Feb 8, 2025)

Executive Summary

Organizations operating in FDA-regulated environments must demonstrate that electronic systems used in regulated processes meet the requirements of **21 CFR Part 11**, including controls over electronic records, electronic signatures, audit trails, and system access. While ServiceNow provides a robust enterprise workflow platform, Part 11 compliance is not achieved through technology alone — it requires **deliberate control design, enforced workflows, and validation-aligned governance**.

This paper explains how organizations can operationalize Part 11 expectations using **ServiceNow Integrated Risk Management (IRM) and Governance, Risk, and Compliance (GRC)** as the control backbone for regulated workflows. It translates regulatory intent into practical ServiceNow design patterns that support:

- Defensible electronic records
- Meaningful electronic signatures
- Secure and traceable audit trails
- Authority checks and role governance
- Ongoing validation alignment

This document is intended for Quality, Compliance, IT, and business stakeholders seeking to use ServiceNow as a controlled system within FDA-regulated operations.

Important Notice: This document describes technical enablement strategies that support regulatory compliance objectives. Final compliance responsibility remains with the regulated organization and its Quality System.

How This Companion Document Fits with the FDA Compliance Framework

Your primary FDA compliance framework establishes how ServiceNow supports:

- GMP and QSR processes
- ITSM and CMDB governance
- Risk management and audit readiness

This companion document narrows focus specifically to:

- **21 CFR Part 11 technical controls**
- Electronic records and electronic signatures
- Evidence integrity and traceability
-

Together, the two papers provide:

Primary FDA Paper	Part 11 Companion
Broad regulatory alignment	Specific electronic record controls
Platform governance	Workflow enforcement
IT process maturity	QA and audit defensibility
Strategic architecture	Operational execution

What 21 CFR Part 11 Requires (in Practical Terms)

While Part 11 is often interpreted as an "IT regulation," its intent is operational:

Regulatory Area	Practical Expectation
System validation (§11.10a)	System supports intended regulated use
Access controls (§11.10d)	Only authorized users can act
Audit trails (§11.10e)	All changes are traceable and immutable
Authority checks (§11.10g)	Approvals are role-appropriate
Electronic signatures (§11.50–70)	Signatures are intentional and attributable
Identity verification (§11.100)	Users cannot repudiate actions

Key Principle:
Part 11 is achieved when **process controls are enforced by system design**, not merely documented in SOPs.

Operationalizing 21 CFR Part 11 in ServiceNow

Rev. January 21, 2026

Electronic Records in ServiceNow

What Constitutes an Electronic Record

Within ServiceNow, regulated electronic records may include:

- Change requests impacting validated systems
- Deviations or quality incidents
- CAPA actions and approvals
- Risk acceptances
- Validation evidence and attachments

If a record supports product quality, patient safety, or regulatory decisions, it may be subject to Part 11 expectations.

Electronic Record Control Design

ServiceNow supports defensible electronic records when the following controls are implemented:

Control Area	ServiceNow Mechanism
Data completeness	Mandatory fields, UI Policies
Data integrity	Dictionary constraints
Change history	sys_audit & sys_history
Record immutability	State-based ACL locking
Attachment traceability	Attachment audit tables
Retention	Table retention policies

Design Pattern: State-Based Record Locking

Once records reach regulatory closure states (e.g., Approved, Implemented, Closed):

- Editing is restricted
- Deletions are prohibited
- Audit history remains available

This ensures post-approval integrity without requiring custom code.

Electronic Signatures: Beyond Simple Approvals

Regulatory Expectations

Electronic signatures must demonstrate:

- Identity of signer
- Intent of action
- Linkage to specific record
- Accountability of signer

Approvals that lack context or accountability may not satisfy audit expectations.

ServiceNow Signature Enforcement Pattern

ServiceNow workflows can support Part 11-aligned electronic signatures when:

Requirement	Implementation
Identity	SSO with MFA
Intent	Explicit approval actions
Signature meaning	Approval rules by role
Non-repudiation	User + timestamp + workflow

Best Practice: Re-authentication on Regulated Approvals

For high-risk regulated workflows, additional credential verification may be enforced during approval to strengthen non-repudiation.

Signature Meaning Matters

Part 11 requires that the meaning of signatures is clear, such as:

- Reviewed
- Approved
- Certified

ServiceNow approval stages and approval types can explicitly encode this meaning into workflow logic and audit records.

Audit Trails and Evidence Integrity

What Auditors Expect

Audit trails must be:

- Automatically generated
- Time-stamped
- Secure from alteration
- Independently stored from user interfaces

ServiceNow Audit Capabilities

Evidence Type	Source Table
Field changes	sys_audit
State transitions	sys_history
Approvals	sysapproval_approver
Attachments	sys_attachment

Together, these form a complete activity chain.

Critical Principle:
Exported spreadsheets or offline approvals do not meet Part 11 expectations because they break traceability and system controls.

Access Control and Authority Checks

Part 11 Control Objectives

Systems must ensure:

- Users only perform permitted actions
- Approvers are appropriately authorized
- Privileged access is governed and reviewed

ServiceNow Role Governance Using IRM/GRC

ServiceNow IRM and GRC modules support:

Control Area	Capability
Role assignments	Policy controls
Access reviews	Periodic certifications
Segregation of duties	Control testing
Privileged monitoring	Continuous monitoring

This allows organizations to demonstrate **preventive controls**, not just detective ones.

Validation Strategy for SaaS Platforms

Shared Responsibility Model

Responsibility	Owner
Platform validation	ServiceNow
Configuration validation	Customer
Intended use validation	Customer

Regulatory validation focuses on whether workflows and controls support intended regulated use, not on the cloud infrastructure itself.

Validation-Aligned Configuration Management

IRM/GRC can track:

- Approved configurations
- Validation status by module
- Change impact assessments
- Re-validation requirements

This prevents configuration drift — a common cause of audit observations in SaaS environments.

Applying Part 11 Controls to Common ServiceNow Processes

Change Management

- Multi-level approvals for regulated systems
- Risk classification based on validation impact
- Post-approval record locking
- Full approval traceability

Incident / Deviation Management

- Controlled closure workflows
- Mandatory root cause documentation
- CAPA linkage enforcement
- Quality review approvals

Risk Acceptance

- Formal acceptance approvals
- Role-based authority
- Evidence retention

These controls convert operational workflows into auditable compliance systems.

Common Audit Findings and How ServiceNow Prevents Them

Audit Observation	Control Strategy
Shared user accounts	Enforced SSO identity
Missing approvals	Workflow gates
Editable closed records	State-based locking
Manual evidence gathering	GRC evidence automation
No impact assessments	IRM risk workflows

Organizations using workflow-enforced controls consistently demonstrate stronger audit outcomes than those relying solely on SOPs.

Why IRM/GRC Is Central to Sustainable Part 11 Compliance

Without governance tooling, compliance becomes:

- Manual
- Reactive
- Audit-driven

With IRM/GRC:

- Controls are embedded in workflows
- Evidence is continuously collected
- Gaps are detected proactively
- Audit readiness becomes operational

This transforms compliance from a periodic project into a continuous operating model.

How Mana'o Pili Delivers Part 11 – Ready ServiceNow

Implementations

Mana'o Pili applies a **Transform-in-Place** methodology focused on:

- Configuration over customization
- Governance before automation
- Validation-aligned design
- Long-term operational sustainability

Our Engagement Approach

1. **Regulatory Workflow Assessment**
   Identify regulated processes and Part 11 applicability.

2. **Control Design Workshops**
   Align quality, IT, and compliance stakeholders.

3. **IRM/GRC Control Mapping**
   Implement preventive and detective controls.

4. **Validation Support Alignment**
   Support CSV documentation and testing strategy.

5. **Operational Readiness Enablement**
   Train teams on sustainable compliance operations.

Our objective is not only regulatory alignment, but **lasting platform maturity that supports business growth without compliance risk**.

Operationalizing 21 CFR Part 11 in ServiceNow

Rev. January 21, 2026

Conclusion

21 CFR Part 11 compliance requires more than audit logs and approvals — it requires **intentional system design that enforces regulated behavior through workflow controls**. ServiceNow, when properly configured and governed using IRM and GRC capabilities, can serve as a compliant operational backbone for regulated processes.

By embedding compliance directly into digital workflows, organizations reduce manual oversight, improve audit readiness, and strengthen data integrity across regulated operations.

With the right architecture and governance, ServiceNow becomes not just a service management platform, but a **validated operational control system**.

About Mana'o Pili

Mana'o Pili is a Hawai'i-based technology consulting firm specializing in business automation through ServiceNow. We partner with organizations to optimize and extend their existing platforms while minimizing customization and reducing long-term technical debt.

We reject one-size-fits-all implementations. Instead, we work closely with our customers — our 'ohana — to design solutions that align with their regulatory, operational, and strategic objectives. Our expertise spans ITSM, ITOM, IRM/GRC, CMDB governance, and compliance-driven service transformation across regulated industries.

Transform-in-Place. Govern with Purpose. Operate with Confidence.