Uncovering Hidden Risks in Veeva Vault PromoMats Configurations: A Security & Compliance Wake-Up Call

Executive Summary

Modern life sciences organizations rely heavily on Veeva Vault PromoMats to manage regulated promotional materials. While PromoMats is a powerful and compliant-ready platform, improper configuration and maintenance, over-permissive access, and missing governance can silently expose organizations to regulatory, legal, and reputational risk.

Risetime's Veeva Certified Associate Administrators have recently seen a wave of security assessments, across multiple deployments, revealing critical system misconfigurations and governance gaps. It is clear that many organizations have not updated their configuration in a way that aligns with their practice, often in environments believed to be "compliant."

This paper highlights real-world missteps, systemic issues, and actionable recommendations to align PromoMats implementations with security and compliance best practices.

The Compliance Threat Is Real and Lurking Beneath the Surface

Many compliance failures due to user error can be remedied with improved configuration:

- Metadata fields allowing circumvention of mandatory workflows
- Outdated or overly permissive user roles and group assignments
- High-risk workflows are enabled for inappropriate users
- Orphaned documents with no assigned owner
- Shared agency accounts lacking individual traceability
- Unmonitored edits to documents post-approval

High-Severity Findings

Overexposed Roles & Permissions

Many users, including agencies, printers, or legacy accounts, are often granted excessive permissions, such as the ability to change source files without PRC visibility, modify metadata post-approval, or even edit system configuration. These permissions are often inherited from poorly maintained group assignments, inappropriate security profile assignments, or outdated document state security settings.

Workflow Gaps and Overrides

In some systems, users were able to bypass critical lifecycle states (e.g., skipping Health Authority Submission steps, and approving Materials) due to non-mandatory field configurations or mis-configured user actions.

Orphaned Content and Manual Ownership Transfer

Documents owned by departed users or agency personnel often remain editable or unowned, leading to accountability gaps and stalled processes.

Shared Logins for Agencies

Shared external accounts obscure the audit trail and make it impossible to determine which individual performed key actions which is a direct violation of best practice for regulated systems.

Expired Materials and Unlinked Components
PromoMats environments commonly contain Materials with expired, unlicensed, or inappropriately licensed Components, many of which are still marked as Approved. These items were not flagged or removed due to missing linkages and/or incomplete Component reviews.

Risks of Inaction

Ignoring these vulnerabilities doesn't make them go away, it amplifies your exposure:

RISK TYPE	IMPACT
Regulatory Fines	PII/PHI leakage or expired Materials in use may trigger HIPAA, GDPR,FDA, etc. penalties.
Audit Failures	Incomplete audit trails, manual/out of system workflows, or untraceable updates often lead to inspection findings.
Reputational Damage	Loss of regulator trust can stall approvals, affect funding, and reduce brand credibility.
Legal Liability	Agencies acting without oversight or outside defined workflows create legal risk for your organization.

What a Proper Optimization and Security Assessment Delivers

Risetime analysts conduct a thorough assessment based on the principles of least privilege and regulatory compliance, transforming your PromoMats system into a secure, auditable asset. Key outcomes include recommendations for:

- **Role Rationalization**: Ensuring users have only the access necessary to perform their duties.
- **Permission Cleanup**: Revoking outdated or inherited permissions that introduce unnecessary risk.
- **Workflow Hardening**: Aligning states, transitions, and field requirements with SOPs and regulatory expectations.
- **Metadata and Document Hygiene**: Cleaning up duplicate or incomplete records that impair traceability.
- **Post-Implementation Governance**: SOPs, training materials, and alerts to ensure long-term integrity.

Conclusion

PromoMats is not inherently risky, but misconfigured environments are. Whether due to organic growth, staff turnover, or lack of governance, most environments drift into risky territory over time. Don't wait for an audit or a warning letter to uncover your blind spots.

A structured optimization and security review from Risetime can be the difference between compliance confidence and catastrophic oversight.

Risk Assessment Overview Examples

Below is a representative sample of anonymized PromoMats configuration risks uncovered in recent assessments, along with recommendations:

High-Risk Configuration Issues

- Agencies had edit rights on MLR/PRC approved Materials, allowing metadata and content changes post-approval.
- Agencies and printers could independently move Materials into an Approved state.
- Documents contained Personally Identifiable Information (PII) like social security numbers and patient ambassador information.

Structural and Process Gaps

- Workflows failed to enforce Health Authority submission fields, allowing circumvention. Components were reused without a Licensing review, leading to unauthorized use.
- Orphaned content remained active after employee offboarding due to missing ownership transfer protocols.

Systemic Governance Weaknesses

- Shared agency accounts masked user-level actions, eliminating individual traceability.
- No unified process to confirm destruction or expiration of Materials in field inventory systems.
- Lack of librarian review allowed for Material dissemination with incomplete links and missing renditions.

Recommendations

- Enforce least-privilege access policies and role-based restrictions.
- Establish mandatory workflows and fields impacting critical approval steps.
- Ensure agencies use versioning and properly link References/Components.
- Implement SOP-driven retirement and expiration processes.
- Track all individual agency access with dedicated user credentials.