

Support regulatory compliance for sensitive data

Use IBM Fusion with HashiCorp Vault to strengthen encryption key governance.



Regulated organizations need to prove more than encryption at rest. Encryption protects data, but key governance controls access. These are two different problems, and regulated environments need to address both.

Encrypting data at rest is now standard practice. But encryption alone does not answer the questions regulators and auditors ask: Who controls the keys? How is access governed? Can you prove key management aligns with your security policies and separation-of-duty requirements?

For platform and security teams, these questions make key governance a requirement, not an option.

Why local key storage may fall short

When keys reside in the same environment as the encrypted data, key control remains tied to the same operational plane. For regulated workloads, that weakens separation of duties and makes governance harder to audit. As environments scale, teams need consistent key governance across infrastructure, not fragmented practices in each storage environment.

The external key management foundation

[IBM Fusion](#) provides an OpenShift-based platform for AI, containers and virtual machines, helping organizations run workloads that require persistent data and strong security controls.

[HashiCorp Vault](#) provides centralized external key management, helping security teams control and govern encryption keys separately from the platform services that use them, while supporting separation of duties, policy enforcement and auditable governance.

Stronger key governance for regulated environments

IBM Fusion environments can use HashiCorp Vault for external encryption key management. Together, they help platform and security teams separate key governance from the storage layer and align encrypted persistent storage with regulatory compliance expectations.¹

Key governance priorities

- **Regulatory alignment.**
Support key management expectations in frameworks such as DORA, PCI DSS and NIST SP 800-57, including documented cryptographic controls, secure key storage and key lifecycle management.
- **Separation of duties.**
Govern encryption keys outside the storage layer, reducing dependency on the same operational plane that stores the encrypted data.
- **Centralized control and audibility.**
Use HashiCorp Vault to centralize key access, policy enforcement and lifecycle practices across infrastructure, with role-based access controls and audit logging for key management operations.

Ready to strengthen key governance? IBM can help you explore external encryption key management for regulated application environments.

[Schedule a session](#)

¹ External KMS integration is supported through IBM Fusion Data Foundation, the foundational data layer for persistent application data on IBM Fusion.

© Copyright IBM Corporation 2026. IBM, and the IBM logo, are trademarks or registered trademarks of IBM Corp., in the U.S. and/or other countries.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.