**Compliance & Legal Alignment**

**What Rules We Need to Follow**

ShopSphere Market is a small online store platform with a payment system and some EU customers. Here are the rules that matter for us:

* **ISO 27001:2022**: A basic security plan to keep things safe and earn trust.
* **PCI DSS v4.0.1**: Needed to protect card payments, started April 2025.
* **GDPR**: Simple rules to handle EU customer info.

**Compliance Matrix**

This table lists the main rules we need, what we’re doing or planning, any issues, and how we’ll fix them. We’ve added a rule for vendors since we use GCP and Visa.

| **Rule (ISO/PCI)** | **What It Means** | **What We Have/Plan** | **Issue** | **Fix Plan** |
| --- | --- | --- | --- | --- |
| **ISO A.5.1** (Policy) | Set up basic security rules. | We check rules twice a year. | No big problems yet. | Next check after holidays, Q4 2025. (Compliance Team) |
| **ISO A.7.2.2** (Training) | Teach staff about safety. | Training once a year. | Not all POS staff trained (Risk PHYS-005). | Start now, add every 3 months, done by Q1 2026. (HR) |
| **ISO A.12.6.1** (Patches) | Fix software weaknesses. | Daily scans, basic firewall. | Old CentOS 7 server (Risk PHYS-001). | Switch to Rocky Linux after peak, Q1 2026. (IT Team) |
| **ISO A.9.2.3** (Access) | Limit who can access systems. | MFA for some admins. | No MFA on desktops/POS (Risk HUM-001). | Add MFA now, focus payment by Q4 2025, all by Q1 2026. (IT Support) |
| **ISO A.12.4.1** (Logging) | Keep track of who does what. | Logs on payment systems. | Weak logging during sales (Risk DB-002). | Improve logs after peak, Q1 2026. (Security Ops) |
| **ISO A.15.1.1** (Vendors) | Check vendors for security. | Basic contract reviews. | No full vendor checks (e.g., GCP) (Risk PHYS-002). | Start email checks now, full plan by Q4 2025. (Compliance Team) |
| **ISO A.13.1.3** (Data Transfer) | Secure data moving around. | TLS 1.2 on main systems. | Old Windows encryption lags (Risk PHYS-002). | Upgrade to TLS 1.3 after peak, Q2 2026. (IT Team) |
| **ISO A.16.1.1** (Incidents) | Handle problems quickly. | Basic response plan. | No way to report breaches (Risk INT-001). | Set up alerts by Q4 2025, test Q1 2026. (Security Ops) |
| **PCI Req 3** (Data) | Keep card data locked. | Basic encryption. | CentOS 7 isn’t safe enough (Risk PHYS-001). | Update server and add protection by Q1 2026. (IT Team) |
| **PCI Req 6** (Updates) | Keep payment system current. | Scans on payment part. | Windows Server lags during busy times (Risk PHYS-002). | Update after peak, Q1 2026. (Security Team) |
| **PCI Req 10** (Tracking) | Track all payment actions. | Some logs in place. | Not all payment moves logged (Risk DB-002). | Add full tracking by Q1 2026. (Security Team) |

*Note: We’ll start overdue tasks (like training, MFA, vendor checks) now since it’s past Q3 2025. Other fixes wait until after busy sales (Q1-Q2 2026).*

**Vendor Plan**

We use vendors like GCP and Visa, so we need to make sure they’re safe. Here’s our plan:

* **Checking Them**: Look at their basic security papers and contracts. Call or email them, especially for payment vendors.
* **Keeping an Eye**: Check their papers once a year starting August 2025, ask for updates every 3 months, and look at logs by hand. Let someone know if there’s a problem.

**Vendor Checklist**

Use this list to check vendors. Mark Yes/No/NA and add notes. Check every year starting August 2025.

| **What to Check** | **What It Means** | **Proof Needed** | **Who Does It** | **Yes/No/NA** | **Notes** |
| --- | --- | --- | --- | --- | --- |
| ISO 27001 Cert | They have a security cert. | Email or paper copy. | Compliance |  | Note if they have it. |
| PCI DSS Cert | Payment vendors have a cert. | Email or proof. | Compliance |  | Check Visa status. |
| Data Agreement | Signed deal for data safety. | Contract or email. | Legal |  | When was it signed? |
| Security Check | Basic safety setup. | Questionnaire or call. | Security |  | Write down results. |
| Incident Plan | Plan for problems. | Email or talk. | Security |  | Note if they have it. |
| Performance Check | They meet goals, no issues. | Emails every 3 months. | IT |  | Last check date. |
| End Plan | They delete data when done. | Contract part or email. | Compliance |  | Confirm or follow up. |
| Sub-Vendor Check | They watch their partners. | Email or statement. | Risk |  | List partners or N/A. |