**📌 GRC360 — Full Basic Features**

**1. Compliance Management**

**Purpose**: Central hub for PCI/ISO requirements tracking.  
**Features**:

* **Framework Library**: PCI DSS 4.0.1 (12 domains, ~300 sub-requirements) and ISO 27001:2022 (93 Annex A controls).
* **Control Explorer**:
  + View controls grouped by domain/Annex.
  + **Search** by control ID, keyword, or tag (e.g., “encryption”, “auth”).
* **CRUD**:
  + **Add**: custom/internal controls.
  + **Update**: annotate or refine requirement wording.
  + **Delete/Archive**: mark control as not applicable.
* **Evidence Linkage**:
  + Attach PDFs, configs, screenshots.
  + Metadata tags (framework, control ID, owner, frequency).
* **Status Tracker**:
  + Mark control as *Compliant*, *Partial*, *Non-Compliant*, *Not Assessed*.
* **Compliance Dashboard**:
  + PCI DSS coverage %.
  + ISO 27001 coverage %.
  + Trend of controls assessed over time.

**Example**:

* PCI DSS 8.2.5 → “Multi-factor authentication is required for all non-console administrative access.”
  + Upload evidence: MFA config screenshot.
  + Status: *Compliant*.
  + Owner: IT Security.

**2. Governance**

**Purpose**: Manage policies and map them to controls.  
**Features**:

* **Policy Library**:
  + Upload or draft policies (e.g., “Access Control Policy.pdf”).
  + Version history with approval workflow.
* **Mapping**:
  + Link each policy to relevant PCI/ISO controls.
* **Review Cycle**:
  + Reminders for annual/semi-annual policy reviews.
* **Access Control**:
  + Only compliance/gov leads can publish policies.

**Example**:

* Policy: “Encryption Policy v1.2” mapped to PCI DSS 3.x and ISO 27001 A.10.1.

**3. Risk Management**

**Purpose**: Turn compliance gaps into risks.  
**Features**:

* **Risk Register**:
  + Add, view, edit, delete risks.
* **Risk Details**:
  + Title, Description, Control reference, Likelihood, Impact, Owner.
* **Risk Scoring**:
  + Basic matrix: *Low, Medium, High*.
* **Linkages**:
  + Risk ↔ Control (PCI/ISO).
  + Risk ↔ Policy.
* **Heatmap Dashboard**:
  + Color-coded matrix (Likelihood × Impact).

**Example**:

* Risk: “Weak MFA coverage.”
  + Linked to PCI DSS 8.2.5.
  + Likelihood: High, Impact: High → Score = Critical.

**4. Evidence Management**

**Purpose**: Store and track compliance evidence.  
**Features**:

* **Repository**:
  + Upload files or links.
  + Tag with control ID, framework, owner.
* **Search/Filter**:
  + By framework, control, file type, or uploader.
* **Versioning**:
  + Keep old evidence with timestamp.
* **Chain of Custody**:
  + Log who uploaded, who viewed, who modified.

**Example**:

* Evidence: “AWS Config export – Sept 2025.csv” linked to PCI DSS 10.2 (logging).

**5. Audit Management**

**Purpose**: Track assessments and findings.  
**Features**:

* **Audit Plans**:
  + Create audit events (e.g., “PCI QSA Assessment 2025”).
* **Task Assignments**:
  + Assign evidence requests to owners.
* **Findings Tracking**:
  + Add/edit audit findings.
  + Link to remediation tasks.
* **Audit History**:
  + Store completed audits, with findings, status, and closure date.

**Example**:

* Audit: PCI QSA – Scope 2025 → Finding: “Missing logs for admin login events” → linked to PCI DSS 10.2.

**6. Dashboard & Reporting**

**Purpose**: Single-pane-of-glass for compliance and risks.  
**Features**:

* **Widgets**:
  + PCI DSS Coverage % (circle graph).
  + ISO 27001 Coverage % (circle graph).
  + Risk Heatmap.
  + Top 5 Non-Compliant Controls.
  + Evidence Activity Log.
* **Export**:
  + Generate PDF/Excel summary reports.
* **Scheduled Reports**:
  + Weekly compliance snapshot via email.

**Example**:

* Dashboard shows PCI DSS coverage: 68%, ISO 27001 coverage: 54%, 3 High risks, 8 open audit findings.

**7. AI Assistant (Basic)**

**Purpose**: Provide instant contextual help.  
**Features**:

* **Search Assistant**:
  + User types: “Show me PCI DSS requirements for MFA.”
  + AI returns: PCI DSS Req 8.2.5 + link to evidence & status.
* **Guided Navigation**:
  + Suggest related risks or evidence.
* **Offline/Local**:
  + Uses small LLM + embeddings of control library.

**8. Audit Logs (System Users)**

**Purpose**: Ensure accountability for solution actions.  
**Features**:

* **Log Events**:
  + Login, file upload, evidence delete, risk update.
* **Immutable Store**:
  + WORM storage, append-only.
* **Search/Export**:
  + Filter logs by user/date/action.

**9. Configurations**

**Purpose**: System administration.  
**Features**:

* User management (add/edit/delete).
* Role-based access control (RBAC).
* Notification policies (email/SMS alerts).
* Integration configs (SIEM, ticketing system).

**10. User Profile**

**Purpose**: Personalization & security.  
**Features**:

* Update profile (name, role, department).
* Notification preferences.
* Enable MFA.
* View personal activity history.

**11. Awareness Module**

**Purpose**: Human factor risk reduction.  
**Features**:

* **Training Library**:
  + Upload courses/videos.
  + Assign training per user/department.
* **Campaigns**:
  + Schedule phishing simulation or awareness campaign.
* **Progress Tracking**:
  + Track completion % and test scores.
* **Compliance Linkage**:
  + Training linked to ISO 27001 A.6.3 (Awareness & training).