# MinRisk User Manual

**Version 1.0** | *Enterprise Risk Management Platform*

---

## Table of Contents



---

## 1. Getting Started

### 1.1 Login

1. Navigate to your organization's MinRisk URL
2. Enter your email address and password
3. Click **Sign In**

### 1.2 User Roles

| Role | Permissions |
|---|---|
| **Admin** | Full access to all modules including user management and configuration |
| **Risk Manager** | Create/edit risks, controls, incidents; view analytics |
| **Viewer** | Read-only access to dashboards and reports |

### 1.3 Navigation

- **Sidebar**: Main navigation tabs for all modules
- **Header**: Organization name, user profile, notifications
- **Sub-tabs**: Each module may have sub-sections (e.g., KRI has Definitions, Data Entry, Alerts)

---

## 2. Dashboard Overview

The Dashboard provides a real-time snapshot of your organization's risk posture.

### 2.1 Key Metrics

| Widget | Description |
|---|---|
| **Total Risks** | Count of all active risks |

| | |
|---|---|
| **High/Critical Risks** | Risks with inherent score ≥16 |
| **Control Coverage** | Percentage of risks with linked controls |
| **Open Incidents** | Unresolved incident count |
| **KRI Breaches** | Active threshold violations |

### 2.2 Risk Distribution Charts

- **By Category**: Pie chart showing risk distribution across categories
- **By Status**: Open, In Progress, Closed breakdown
- **Heat Map Preview**: Quick view of likelihood × impact matrix

---

## 3. Risk Management

### 3.1 Risk Register

The Risk Register is your central repository for all identified risks.

**Viewing Risks:**

1. Click **Risks** tab
2. Use filters to narrow by Category, Status, Owner, Division, or Department
3. Click any risk row to view full details

**Risk Properties:**

- **Risk Code**: Auto-generated (e.g., CRE-OPS-001)
- **Risk Title**: Brief descriptive name
- **Risk Description**: Detailed statement following "The risk that..." format
- **Category/Sub-category**: From your organization's taxonomy
- **Owner**: Responsible person
- **Division/Department**: Organizational unit
- **Inherent Score**: Likelihood × Impact (before controls)
- **Residual Score**: After control effectiveness applied

### 3.2 Creating a New Risk

**Workflow: Create Risk**

```
Step 1: Click "Add Risk" button
     ↓
Step 2: Select Category from dropdown
     ↓
Step 3: Select Sub-Category
     ↓
Step 4: (Optional) Use AI Classification
         - Enter free-text risk statement
         - Click "Classify with AI"
         - AI suggests category & refined statement
     ↓
Step 5: Fill required fields:
         - Risk Title
```

```
         - Risk Description
         - Division & Department
         - Risk Owner
    ↓
Step 6: Score Inherent Risk:
         - Likelihood (1–5)
         - Impact (1–5)
    ↓
Step 7: (Optional) Link Controls
         - Select from Control Library
         - Or create new control inline
    ↓
Step 8: Click "Create Risk"
```

### 3.3 Risk Scoring Matrix

| Score | Likelihood | Impact |
|---|---|---|
| 1 | Rare | Negligible |
| 2 | Unlikely | Minor |
| 3 | Possible | Moderate |
| 4 | Likely | Major |
| 5 | Almost Certain | Catastrophic |

**Risk Rating:**

- **Low (1-4)**: Green - Acceptable
- **Medium (5-9)**: Yellow - Monitor
- **High (10-15)**: Orange - Action required
- **Critical (16-25)**: Red - Immediate attention

### 3.4 Editing & Deleting Risks

- **Edit**: Click risk row → Modify fields → Save
- **Delete**: Click risk row → Delete (unlinking controls/KRIs, not deleting)

---

## 4. Control Management

### 4.1 Control Register

Controls are the mechanisms used to mitigate risks.

**Control Types:**

| Type | Description |
|---|---|
| **Preventive** | Stops risk events from occurring |
| **Detective** | Identifies risk events that occurred |
| **Corrective** | Remedies impact after occurrence |

**Control Target:**

- **Likelihood**: Reduces probability of occurrence
- **Impact**: Reduces severity if event occurs
- **Both**: Affects both dimensions

### 4.2 DIME Framework

Controls are assessed using the **DIME** methodology:

| Component | Description | Score (0-3) |
|---|---|---|
| **D** - Design | How well is the control designed? | 0=None, 3=Strong |
| **I** - Implementation | Is it fully implemented? | 0=None, 3=Full |
| **M** - Monitoring | Is there ongoing oversight? | 0=None, 3=Continuous |
| **E** - Evaluation | Is it regularly tested? | 0=None, 3=Regular |

**Effectiveness Formula:**

```
Effectiveness = (D + I + M + E) / 12 × 100%
```

### 4.3 Creating a Control

**Workflow: Create Control**

```
Step 1: Navigate to Controls tab
    ↓
Step 2: Click "Add Control"
    ↓
Step 3: Enter details:
         - Control Name
         - Description
         - Control Type (Preventive/Detective/Corrective)
         - Target (Likelihood/Impact/Both)
    ↓
Step 4: Score DIME components (0-3 each)
    ↓
Step 5: Click "Create Control"
    ↓
Step 6: Link to Risks (optional)
         - Select risks that this control mitigates
```

### 4.4 Residual Risk Calculation

When controls are linked, residual risk is calculated:

```
Residual = Inherent - (Inherent - 1) × Max Effectiveness
```

Example: Inherent 5, Control 75% effective → Residual = 5 - (4 × 0.75) = 2

---

## 5. Incident Management

### 5.1 Overview

Track risk events, near-misses, and operational failures.

**Incident Status:**

- **Open**: New incident awaiting investigation
- **Under Investigation**: Being analyzed
- **Resolved**: Root cause addressed
- **Closed**: Fully remediated

### 5.2 Logging an Incident

**Workflow: Log Incident**

```
Step 1: Navigate to Incidents tab
    ↓
Step 2: Click "Log Incident"
    ↓
Step 3: Complete form:
         - Incident Title
         - Description (what happened)
         - Incident Type (select or custom)
         - Date Occurred
         - Reported By (auto-filled)
    ↓
Step 4: (Optional) Attach supporting documents
    ↓
Step 5: Click "Submit"
         → Incident Code auto-generated (INC-001)
```

### 5.3 Incident-to-Risk Mapping

Link incidents to existing risks for trend analysis:

**Manual Mapping:**

1. Open incident details
2. Click "Link to Risk"
3. Select risk from dropdown
4. Add mapping notes

**AI-Assisted Mapping:**

1. Click "Analyze with AI"
2. Review AI suggestions (includes confidence score)
3. Accept or reject each suggestion
4. AI explains reasoning for each match

### 5.4 Root Cause Analysis

For each incident, document:

- **Root Causes**: Underlying factors
- **Contributing Factors**: Secondary causes
- **Lessons Learned**: Preventive measures
- **Corrective Actions**: Remediation steps

---

# 6. AI Risk Generator

## 6.1 AI-Powered Risk Generation

Generate comprehensive risks using AI:

**Workflow: AI Risk Generation**

```
Step 1: Navigate to AI tab
    ↓
Step 2: Configure generation:
         - Industry (e.g., Banking, Healthcare)
         - Business Unit
         - Category (or All Categories)
         - Number of Risks (1-10)
         - Additional Context (optional)
    ↓
Step 3: Click "Generate Risks"
    ↓
Step 4: Review generated risks:
         - Risk statement
         - Suggested category
         - Preliminary scoring
         - Rationale
    ↓
Step 5: For each:
         - Accept → Added to Risk Register
         - Reject → Discarded
         - Edit → Modify before saving
```

## 6.2 AI Control Recommendations

For any risk, get AI-suggested controls:

1. Open risk details
2. Click "Get AI Control Recommendations"
3. Review suggestions with:
    - Control name and description
    - Type (Preventive/Detective/Corrective)
    - Suggested DIME scores
    - Implementation rationale
4. Accept to create control and link automatically

## 6.3 Risk Statement Refinement

Polish risk statements with AI:

1. In risk form, enter draft statement

2. Click "Fine-tune with AI"
3. AI provides:
    - Refined professional statement
    - List of improvements made
    - Explanation of changes

---

# 7. Analytics & Reporting

### 7.1 Risk Heat Map

Interactive likelihood × impact matrix:

- **Click quadrant**: Filter risks in that zone
- **Hover**: See risk count and details
- **Export**: Download as image or PDF

### 7.2 Trend Analysis

Track risk metrics over time:

- **Risk Count Trends**: New vs. closed risks
- **Category Distribution**: Changes by category
- **Score Movements**: Inherent/residual trending

### 7.3 Reports

| Report | Description |
|---|---|
| **Risk Register Export** | Full risk listing with controls |
| **Control Effectiveness** | DIME scores and coverage |
| **Incident Summary** | Monthly/quarterly incident stats |
| **KRI Dashboard** | All indicators with breach status |

---

# 8. KRI/KCI Management

### 8.1 KRI Definitions

Key Risk Indicators are quantitative metrics for proactive monitoring.

**Indicator Types:**

| Type | Description |
|---|---|
| **Leading** | Predictive indicators (warn before event) |
| **Lagging** | Historical indicators (confirm after event) |
| **Concurrent** | Real-time indicators |

### 8.2 Creating a KRI

**Workflow: Create KRI**

```
Step 1: Navigate to KRI/KCI → Definitions
    ↓
Step 2: Click "Add KRI"
    ↓
Step 3: Configure:
         - KRI Name
         - Description
         - Measurement Unit (%, count, $)
         - Data Source
         - Collection Frequency
    ↓
Step 4: Set Thresholds:
         - Target Value
         - Lower Threshold (Yellow)
         - Upper Threshold (Red)
         - Direction (Above/Below/Between)
    ↓
Step 5: Assign Responsible User
    ↓
Step 6: Link to Risks (optional)
    ↓
Step 7: Click "Create"
         → KRI Code auto-generated (KRI-001)
```

### 8.3 Data Entry

Record actual values:

1. Navigate to KRI/KCI → Data Entry
2. Select KRI from list
3. Enter:
    - Measurement Date
    - Actual Value
    - Data Quality (Verified/Estimated/Provisional)
    - Notes
4. Click "Submit"
    - Alert status auto-calculated (Green/Yellow/Red)

### 8.4 KRI Alerts

When thresholds are breached, alerts are created:

**Alert Lifecycle:**

```
Open → Acknowledged → Resolved
                   → Dismissed (if false positive)
```

**Responding to Alerts:**

1. Navigate to KRI/KCI → Alerts
2. View open alerts

3. Click alert to:
    - Review details and history
    - Add notes
    - Acknowledge (confirm awareness)
    - Resolve (remediation complete)

---

# 9. Risk Intelligence

## 9.1 External Events

Monitor external risk events that may impact your organization.

**Sources:**

- RSS feeds from regulatory bodies
- News aggregators
- Industry publications
- Custom sources

## 9.2 Configuring RSS Sources

**Workflow: Add RSS Source**

```
Step 1: Navigate to Intelligence → RSS Sources
    ↓
Step 2: Click "Add Source"
    ↓
Step 3: Enter:
         - Source Name
         - RSS Feed URL
         - Category (optional)
    ↓
Step 4: Click "Save"
    ↓
Step 5: Click "Scan Now" to fetch events
```

## 9.3 Risk Keywords

Define keywords that trigger relevance matching:

1. Navigate to Intelligence → Risk Keywords
2. Add keywords (e.g., "cybersecurity breach", "regulatory fine")
3. Events matching keywords get higher relevance scores

## 9.4 Intelligence Alerts

When external events are relevant to your risks:

**Workflow: Process Intelligence Alert**

```
Alert Created (AI analyzed event)
    ↓
Review in Alerts tab:
    - Event summary
```

```
    – Matched risk
    – AI confidence score
    – Suggested likelihood/impact changes
    ↓
Decision:
    Accept → Risk scores updated automatically
    Reject → Alert dismissed
    ↓
(Optional) Add notes explaining decision
```

---

## 10. Administration

*Admin access required*

### 10.1 Risk Taxonomy

Configure your organization's risk classification:

1. Navigate to Admin → Risk Taxonomy
2. Manage:
    - Categories (e.g., Operational, Financial, Compliance)
    - Sub-categories per category
    - Descriptions for guidance

### 10.2 Risk Configuration

Set organizational parameters:

| Setting | Description |
|---|---|
| **Divisions** | Top-level organizational units |
| **Departments** | Sub-units within divisions |
| **Impact Scale** | 1-5 scale descriptors |
| **Likelihood Scale** | 1-5 scale descriptors |
| **Default Period** | Active risk assessment period |

### 10.3 Appetite & Tolerance

Define risk boundaries:

**Risk Appetite Statement:**

- Version-controlled document
- Board approval tracking
- Effective date ranges

**Tolerance Metrics:**

- Per-category thresholds
- Metric types: Range, Maximum, Minimum, Directional
- Automatic breach detection

### 10.4 User Management

Manage system users:

**Workflow: Invite User**

```
Step 1: Navigate to Admin → User Management
    ↓
Step 2: Click "Invite User"
    ↓
Step 3: Enter:
         - Email address
         - Role (Admin/Risk Manager/Viewer)
         - Division/Department access
    ↓
Step 4: Click "Send Invitation"
         → User receives email with setup link
```

---

## 11. Common Workflows

### 11.1 Complete Risk Assessment Workflow

```
1. IDENTIFY RISKS
   - Use AI Generator for initial population
   - Manual entry for specific risks
   - Review and classify using taxonomy

2. ASSESS RISKS
   - Score inherent likelihood and impact
   - Document risk descriptions and owners
   - Link to relevant KRIs

3. EVALUATE CONTROLS
   - Identify existing controls
   - Score using DIME framework
   - Calculate residual risk

4. MONITOR
   - Set up KRIs for key risks
   - Enter measurement data regularly
   - Respond to breaches/alerts

5. REPORT
   - Generate analytics reports
   - Review heat maps and trends
   - Present to stakeholders

6. REVIEW
   - Periodic reassessment
   - Update controls as needed
   - Close mitigated risks
```

### 11.2 Incident Response Workflow

```
1. LOG
   - Immediately log incident
   - Capture key details

2. ASSESS
   - Determine severity
   - Assign investigation lead

3. INVESTIGATE
   - Root cause analysis
   - Link to existing risks

4. REMEDIATE
   - Implement corrective actions
   - Update controls if needed

5. CLOSE
   - Document lessons learned
   - Update risk register
```

### 11.3 Daily Risk Manager Routine

```
Morning:
□ Check KRI Alerts dashboard
□ Review pending Intelligence Alerts
□ Check open incidents status

Ongoing:
□ Update KRI measurements
□ Process new risk submissions
□ Review control effectiveness

Weekly:
□ Run analytics reports
□ Update risk assessments
□ Team sync on high-priority risks
```

---

## Quick Reference

### Keyboard Shortcuts

| Action | Shortcut |
|---|---|
| Search | Ctrl/Cmd + K |
| Save | Ctrl/Cmd + S |
| Refresh | F5 |

### Contact Support

For technical issues or questions:

- Email: support@minrisk.io
- Documentation: docs.minrisk.io

---