### Frontend Components

#### SMS Management

* PersonaManagement - Interface for managing personnel data
* TrainingRecordsList - List and management of training records
* CertificationTracker - Dashboard for tracking certification status
* ComplianceOverview - Summary of compliance status
* ConsentManagement - Interface for managing GDPR consents
* **Task 1.1.1**: Design GDPR-compliant user data schema
* **Task 1.1.2**: Create data models for personas, training records, and certifications
* **Task 1.1.3**: Implement data anonymization and pseudonymization utilities
* **Technical Requirements**:
  + PostgreSQL with encryption extensions
  + Data masking and anonymization libraries
  + GDPR consent tracking mechanisms
  + Unit tests for privacy-related functions

Here's the expanded schema integrating all requested ISO standards, with **applicability markers**:

* **Q**: ISO 9001:2015 (Quality)
* **E**: ISO 14001:2015 (Environmental)
* **S**: ISO 45001:2018 (OH&S)
* **I**: ISO/IEC 27001:2022 (Information Security)
* **A**: ISO/IEC 42001:2023 (AI Management)
* **SR**: ISO 26000:2010 (Social Responsibility)
* **En**: ISO 50001:2018 (Energy)

### **1. Organization & Context**

| **Field** | **Type** | **Applicability** | **Description** |
| --- | --- | --- | --- |
| org\_name | Text | All | Organization name |
| scope\_qms | Text | Q | Scope of QMS |
| scope\_ems | Text | E | Scope of EMS |
| scope\_ohs | Text | S | Scope of OH&S |
| **scope\_isms** | Text | I | Scope of ISMS (ISO 27001) |
| **scope\_aims** | Text | A | Scope of AIMS (ISO 42001) |
| **scope\_energy** | Text | En | Scope of EnMS (ISO 50001) |
| interested\_parties | JSON | All | Stakeholders (customers, regulators, communities) |
| internal\_issues | Text | All | Internal challenges (resources, culture, etc.) |
| external\_issues | Text | All | External challenges (regulations, market, etc.) |
| **sr\_context** | Text | SR | Social responsibility context |
| **ai\_system\_inventory** | JSON | A | List of AI systems in use (ISO 42001) |

### **2. Leadership & Commitment**

| **Field** | **Type** | **Applicability** | **Description** |
| --- | --- | --- | --- |
| quality\_policy | Text | Q | Quality policy |
| environmental\_policy | Text | E | Environmental policy |
| ohs\_policy | Text | S | OH&S policy |
| **infosec\_policy** | Text | I | Information security policy |
| **ai\_governance\_policy** | Text | A | AI management policy |
| **energy\_policy** | Text | En | Energy management policy |
| **sr\_commitment** | Text | SR | Social responsibility commitment |
| roles\_responsibilities | JSON | All | Roles with assigned responsibilities |
| mgmt\_commitment\_evidence | Text | All | Proof of leadership involvement |

### **3. Planning**

#### **3.1. Risks & Opportunities**

| **Field** | **Type** | **Applicability** | **Description** |
| --- | --- | --- | --- |
| risk\_id | ID | All | Unique risk identifier |
| risk\_category | Enum | All | Quality, Environmental, OH&S, Infosec, AI, Energy, Social |
| risk\_source | Enum | All | Process, Supplier, Legal, Cyber, Bias, Community |
| **ai\_risk\_type** | Enum | A | Bias, Security, Transparency, Safety (ISO 42001) |
| **infosec\_asset** | Text | I | Affected asset (data, system) |
| risk\_impact | Enum | All | Critical, High, Medium, Low |
| mitigation\_plan | Text | All | Action plan to address risk |

#### **3.2. Objectives & Targets**

| **Field** | **Type** | **Applicability** | **Description** |
| --- | --- | --- | --- |
| objective\_id | ID | All | Unique objective ID |
| objective\_type | Enum | All | Quality, Env, OH&S, Infosec, AI, Energy, Social |
| **energy\_target** | Float | En | Energy consumption target (kWh) |
| **ai\_ethics\_kpi** | Text | A | AI ethics KPI (e.g., "Bias reduction rate") |
| target\_value | Float | All | Numerical target value |
| deadline | Date | All | Target completion date |

#### **3.3. Legal & Other Requirements**

| **Field** | **Type** | **Applicability** | **Description** |
| --- | --- | --- | --- |
| requirement\_id | ID | All | Unique requirement ID |
| requirement\_standard | Enum | All | Q, E, S, I, A, En, SR |
| regulation\_type | Enum | All | GDPR, NIST, Cybersecurity Law, Labor Law |
| **ai\_ethics\_standard** | Text | A | AI ethics framework applied |
| compliance\_status | Enum | All | Compliant, Non-Compliant, Pending |

### **4. Support**

#### **4.1. Resources & Competence**

| **Field** | **Type** | **Applicability** | **Description** |
| --- | --- | --- | --- |
| training\_record\_id | ID | All | Training session ID |
| **infosec\_cert\_level** | Enum | I | CISSP, CISM, CompTIA Security+ |
| **ai\_competency** | Enum | A | AI Ethics, ML Ops, Bias Mitigation |
| **energy\_auditor\_cert** | Text | En | Energy auditor certification number |
| competency\_status | Enum | All | Qualified, In Training, Needs Evaluation |

#### **4.2. Awareness & Communication**

| **Field** | **Type** | **Applicability** | **Description** |
| --- | --- | --- | --- |
| comm\_id | ID | All | Communication record ID |
| comm\_channel | Enum | All | Email, Meeting, Dashboard, Training |
| **privacy\_notice** | Boolean | I, A | Privacy notice communicated (Y/N) |
| **sr\_awareness** | Boolean | SR | Social responsibility awareness done |

#### **4.3. Documented Information**

| **Field** | **Type** | **Applicability** | **Description** |
| --- | --- | --- | --- |
| doc\_id | ID | All | Document ID |
| doc\_category | Enum | All | Policy, Procedure, Record, AI Model Card |
| **access\_control\_level** | Enum | I, A | Public, Restricted, Confidential |
| **energy\_monitoring\_log** | Text | En | Energy consumption log location |

### **5. Operations**

#### **5.1. Operational Controls**

| **Field** | **Type** | **Applicability** | **Description** |
| --- | --- | --- | --- |
| process\_id | ID | All | Unique process ID |
| **infosec\_controls** | JSON | I | Encryption, MFA, Access logs (ISO 27001) |
| **ai\_bias\_controls** | Text | A | Bias detection methods (ISO 42001) |
| **energy\_consumption** | Float | En | Real-time energy usage (kWh) |
| **community\_impact** | Text | SR | Community engagement actions |

#### **5.2. Emergency Preparedness**

| **Field** | **Type** | **Applicability** | **Description** |
| --- | --- | --- | --- |
| emergency\_id | ID | E,S,I,A | Emergency scenario ID |
| **cyber\_incident\_type** | Enum | I | Breach, Ransomware, DDoS |
| **ai\_failure\_scenario** | Enum | A | Bias Incident, Safety Failure, Data Poisoning |
| response\_plan | Text | E,S,I,A | Response steps |

### **6. Performance Evaluation**

#### **6.1. Monitoring & Measurement**

| **Field** | **Type** | **Applicability** | **Description** |
| --- | --- | --- | --- |
| metric\_id | ID | All | Unique metric ID |
| **security\_metrics** | JSON | I | Incident Rate, Patch Time, Phishing Test Pass |
| **ai\_performance** | JSON | A | Accuracy, Fairness Score, Drift Detection |
| **carbon\_footprint** | Float | E, En | CO2 emissions (tons) |
| **sr\_compliance\_score** | Float | SR | Social responsibility score |

#### **6.2. Internal Audit**

| **Field** | **Type** | **Applicability** | **Description** |
| --- | --- | --- | --- |
| audit\_standard | Enum | All | QMS, EMS, OH&S, ISMS, AIMS, EnMS, SR |
| **infosec\_test\_results** | Text | I | Penetration test results |
| **ai\_system\_audit** | Text | A | AI system validation report |
| **energy\_efficiency\_audit** | Text | En | Energy performance report |

### **7. Improvement**

#### **7.1. Nonconformity & Corrective Action**

| **Field** | **Type** | **Applicability** | **Description** |
| --- | --- | --- | --- |
| nc\_source | Enum | All | Audit, Complaint, Cyber Incident, AI Failure |
| **data\_breach\_details** | Text | I | PII records affected |
| **ai\_incident\_root\_cause** | Text | A | Root cause of AI failure |
| **energy\_waste\_source** | Text | En | Source of energy inefficiency |

#### **7.2. Incident Management**

| **Field** | **Type** | **Applicability** | **Description** |
| --- | --- | --- | --- |
| incident\_category | Enum | All | OH&S, Environmental, Infosec, AI, Energy |
| **cyber\_incident\_severity** | Enum | I | Catastrophic, Major, Minor (NIST Scale) |
| **ai\_impact\_level** | Enum | A | Individual, Group, Societal |
| **community\_impact\_level** | Enum | SR | Local, Regional, National |

### **Key Enhancements**

1. **Cross-Standard Linkages**:
   * Risks → Objectives (Many-to-Many)
   * Nonconformities → Corrective Actions (1-to-1)
   * Processes → Controls (1-to-Many)
   * AI Systems ↔ Infosec Controls (Bidirectional)
2. **New Modules**:
   * **AI Governance**: Model cards, bias controls, ethics KPIs
   * **Energy Management**: Real-time monitoring, efficiency audits
   * **Social Responsibility**: Community impact assessments
   * **Integrated Risk**: Cyber-physical risk mapping
3. **Automation Features**:
   * AI drift detection alerts
   * Energy consumption forecasting
   * Automated compliance dashboards
   * Cross-standard gap analysis reports
4. **Evidence Management**:
   * Blockchain-based document integrity (ISO 27001)
   * AI training data versioning (ISO 42001)
   * Energy calibration certificates (ISO 50001)

### **Implementation Strategy**

Diagram

Code

Download

Single Portal

ISO Modules

QMS

EMS

OH&S

ISMS

AIMS

EnMS

SR

Unified Database

Relational: PostgreSQL

Document: MongoDB

AI Engine

Risk Prediction

Auto-Compliance

**Database Recommendations**:

* **PostgreSQL**: For transactional data (audits, incidents)
* **MongoDB**: For unstructured data (policies, risk assessments)
* **TimeScaleDB**: For energy/emissions time-series data

**Compliance Automation**:

* NLP for regulation updates
* Smart contracts for evidence chain-of-custody
* API integrations with:
  + Energy monitoring systems
  + Security information tools (SIEM)
  + AI monitoring platforms

This integrated schema supports all 7 ISO standards while maintaining the Annex SL structure. Custom fields can be added per organizational needs without disrupting core compliance tracking.

[ISO 9001:2015](https://www.iso.org/standard/62085.html)

Quality management systems — Requirements

[Reference number](https://www.iso.org/standard/27001)

[ISO/IEC 27001:2022](https://www.iso.org/standard/27001)

[© ISO 2025](https://www.iso.org/standard/27001)

[Edition 3](https://www.iso.org/standard/27001)

[2022-10](https://www.iso.org/standard/27001)

[ISO/IEC 27001:2022](https://www.iso.org/standard/27001)

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

[Reference number](https://www.iso.org/standard/81230.html)

[ISO/IEC 42001:2023](https://www.iso.org/standard/81230.html)

[2023-12](https://www.iso.org/standard/81230.html)

[ISO/IEC 42001:2023](https://www.iso.org/standard/81230.html)

Information technology — Artificial intelligence — Management system

[ISO 45001:2018](https://www.iso.org/standard/63787.html)

Occupational health and safety management systems — Requirements with guidance for use

[ISO 14001:2015](https://www.iso.org/standard/60857.html)

Environmental management systems — Requirements with guidance for use

[ISO 26000:2010](https://www.iso.org/standard/42546.html)

Guidance on social responsibility

[ISO 50001:2018](https://www.iso.org/standard/69426.html)

Energy management systems — Requirements with guidance for use

* **Task 1.4.1**: Integrate persona management with training records
* **Task 1.4.2**: Implement compliance checking for training requirements
* **Task 1.4.3**: Create basic reporting for training status
* **Task 1.4.4**: Conduct end-to-end testing
* **Deliverable**: MVP with basic SMS persona management
  + GDPR-compliant user management
  + Training record tracking
  + Certification management
  + Basic compliance reporting
* GET /api/sms/personas - List all personas (with privacy filters)
* POST /api/sms/personas - Create new persona
* GET /api/sms/personas/:id - Get persona details
* PUT /api/sms/personas/:id - Update persona
* DELETE /api/sms/personas/:id - Delete/anonymize persona
* GET /api/sms/training-records - List training records
* POST /api/sms/training-records - Add training record
* GET /api/sms/certifications - List certifications
* POST /api/sms/certifications - Add certification type
* GET /api/sms/compliance-status - Get compliance overview
* **Task 2.2.1**: Design document management architecture
  + Define document metadata schema
  + Create document classification system
  + Design version control workflow
  + Develop access control model
* create directories and files as required

### SMS Management: Document Management System

* **Task 2.2.2**: Implement document storage and retrieval
  + Create secure document repository
  + Develop metadata indexing
  + Implement full-text search
  + Build document preview functionality
* create directories and files as required

#### Week 8

### SMS Management: Document Management System

* **Task 2.2.3**: Develop document workflow system
  + Create approval workflows
  + Implement review cycles
  + Develop expiration and renewal tracking
  + Build document linking and relationships
* create directories and files as required

### SMS Management: Document Management System

* **Task 2.2.4**: Implement document compliance features
  + Create document retention policies
  + Develop automatic archiving
  + Implement audit trail for document access
  + Build compliance reporting for documentation
* create directories and files as required

### SMS Management: Document Management System

**Technical Requirements**:

* S3 or equivalent for document storage
* Elasticsearch for full-text search
* PDF.js for document preview
* Workflow engine for approval processes
* create directories and files as required
* **Task 2.3.1**: Design audit logging system
  + Define audit event schema
  + Create logging architecture
  + Design retention policies
  + Develop access control model

### SMS Management: Audit Trail and Compliance Logging

* **Task 2.3.2**: Implement comprehensive event logging
  + Create centralized logging service
  + Develop context-aware logging
  + Implement user action tracking
  + Build system event logging

### SMS Management: Audit Trail and Compliance Logging

* **Task 2.3.3**: Develop audit review interface
  + Create audit log viewer
  + Implement filtering and search
  + Develop export functionality
  + Build anomaly highlighting

### SMS Management: Audit Trail and Compliance Logging

* **Task 2.3.4**: Implement compliance reporting
  + Create compliance audit reports
  + Develop evidence collection
  + Implement audit trail verification
  + Build tamper detection

### SMS Management: Audit Trail and Compliance Logging

**Technical Requirements**:

* ELK stack (Elasticsearch, Logstash, Kibana)
* Immutable logging with timestamps
* Digital signatures for log integrity
* SIEM integration capabilities

### SMS Management: Fully Compliant SMS Management System

#### Week 11

* **Task 2.4.1**: Integrate incident reporting with document management
  + Connect incidents to relevant documents
  + Develop document-based incident resolution
  + Implement evidence collection workflow
  + Build document-driven notifications

## Integration and Deliverable Completion

### SMS Management: Fully Compliant SMS Management System

* **Task 2.4.2**: Enhance audit trails with document tracking
  + Create document access audit logs
  + Develop document lifecycle tracking
  + Implement compliance verification
  + Build comprehensive audit reports

## Integration and Deliverable Completion

### SMS Management: Fully Compliant SMS Management System

* **Task 2.4.3**: Implement advanced compliance features
  + Create compliance dashboards
  + Develop regulatory reporting automation
  + Implement compliance calendar
  + Build compliance risk assessment

## Integration and Deliverable Completion

### SMS Management: Fully Compliant SMS Management System

* **Task 2.4.4**: Finalize and test full system
  + Conduct end-to-end testing
  + Perform security and compliance review
  + Optimize performance
  + Create user documentation

## Integration and Deliverable Completion

### SMS Management: Fully Compliant SMS Management System

**Deliverable**: Fully compliant SMS management system

* NIS2-compliant incident reporting with authority notification
* Comprehensive document management with version control
* Detailed audit trails and compliance logging
* Automated compliance reporting and verification
* Integrated risk assessment and management
* **Task 4.1.1**: Design risk assessment framework
  + Define risk categories and scoring methodology
  + Create risk factor identification system
  + Design automated assessment workflows
  + Develop risk visualization components
* **SMS Management: Risk Assessment Automation**
* **Task 4.1.2**: Implement risk data collection
  + Create risk factor data collectors
  + Develop integration with incident database
  + Implement external threat intelligence feeds
  + Build compliance requirement mapping

**SMS Management: Risk Assessment Automation**

* **Task 4.1.3**: Implement risk assessment engine
  + Create risk scoring algorithms
  + Develop automated assessment workflows
  + Implement risk trend analysis
  + Build risk correlation engine
* **Task 4.1.4**: Implement risk management interface
  + Create risk dashboard with visualizations
  + Develop risk detail and drill-down views
  + Implement risk mitigation planning
  + Build risk tracking and monitoring

**Technical Requirements**:

* Rule engine for risk scoring
* Machine learning for risk pattern recognition
* Integration with threat intelligence APIs
* Risk visualization components
* Workflow engine for assessment automation
* **SMS Management: Training Recommendation Engine**
* **Task 4.2.1**: Design recommendation engine architecture
  + Define recommendation algorithms
  + Create user profiling system
  + Design training content metadata schema
  + Develop recommendation visualization

**Week 20**

* **SMS Management: Training Recommendation Engine**
* **Task 4.2.2**: Implement user profiling
  + Create skill gap analysis
  + Develop learning history tracking
  + Implement role-based requirement mapping
  + Build interest and preference modeling
* **SMS Management: Training Recommendation Engine**
* **Task 4.2.3**: Implement recommendation algorithms
  + Create collaborative filtering system
  + Develop content-based recommendations
  + Implement hybrid recommendation approach
  + Build personalized learning paths
* **SMS Management: Training Recommendation Engine**
* **Task 4.2.4**: Implement recommendation interface
  + Create personalized training dashboard
  + Develop recommendation explanation
  + Implement training plan builder
  + Build progress tracking and analytics
* **SMS Management: Training Recommendation Engine**

**Technical Requirements**:

* Recommendation algorithms (collaborative filtering, content-based)
* User profiling system
* Training content metadata schema
* Learning path generation
* Personalized dashboard components
* **SMS Management: Compliance Forecasting**
* **Task 4.3.2**: Implement compliance data analysis
  + Create historical compliance data analysis
  + Develop compliance pattern recognition
  + Implement leading indicator identification
  + Build compliance risk scoring
* **SMS Management: Compliance Forecasting**
* **Task 4.3.3**: Implement forecasting models
  + Create time series forecasting for compliance metrics
  + Develop scenario-based forecasting
  + Implement what-if analysis tools
  + Build confidence interval calculation
* **SMS Management: Compliance Forecasting**
* **Task 4.3.4**: Implement forecasting interface
  + Create compliance forecast dashboard
  + Develop trend visualization
  + Implement intervention planning tools
  + Build forecast accuracy tracking
* **SMS Management: Compliance Forecasting**

**Technical Requirements**:

* Time series forecasting models
* Pattern recognition algorithms
* Scenario modeling engine
* Interactive forecast visualization
* Intervention recommendation system

**SMS Management: Intelligent SMS Management with Predictive Capabilities**

* **Task 4.4.1**: Integrate risk assessment with training recommendations
  + Connect risk factors to training needs
  + Develop risk-based training prioritization
  + Implement skill gap analysis based on risk assessment
  + Build integrated risk mitigation through training
* **Task 4.4.2**: Integrate training recommendations with compliance forecasting
  + Connect compliance forecasts to training plans
  + Develop proactive compliance training
  + Implement training effectiveness prediction
  + Build comprehensive SMS intelligence dashboard
* **Task 4.4.3**: Finalize and test SMS management system
  + Conduct end-to-end testing
  + Perform security and compliance review
  + Optimize performance
  + Create user documentation

**Deliverable**: Intelligent SMS management with predictive capabilities

* Automated risk assessment with scoring and trending
* Personalized training recommendation engine
* Compliance forecasting with intervention planning
* Integrated SMS intelligence dashboard

**Machine Learning and AI Components**

**Predictive Models**

* Time series forecasting (ARIMA, Prophet, LSTM)
* Classification models for risk assessment
* Regression models for impact prediction
* Reinforcement learning for optimization
* Recommendation systems for training

**Data Processing Pipeline**

* ETL processes for model training data
* Feature engineering and selection
* Data validation and quality assurance
* Model training and evaluation
* Model deployment and serving

**Optimization Algorithms**

* Constraint satisfaction problems
* Genetic algorithms for complex scheduling
* Multi-objective optimization
* Resource allocation algorithms
* Route optimization

**Integration Architecture**

**Cross-Application Data Flow**

* Event-driven updates between applications
* Shared data models for integrated analytics
* API gateway for cross-application requests
* Unified dashboard for comprehensive insights

**AI Service Layer**

* Centralized model serving infrastructure
* Batch and real-time prediction APIs
* Model monitoring and retraining
* Feature store for shared features
* Explanation service for model interpretability

**User Interface Components**

**Advanced Visualization**

* Interactive forecasting charts
* Risk heatmaps and dashboards
* Resource optimization visualizations
* Weather impact maps
* Maintenance scheduling calendars

**Decision Support Tools**

* What-if analysis interfaces
* Scenario comparison tools
* Recommendation explanations
* Alert management and prioritization
* Intervention planning assistants

**Implementation Approach**

**Development Methodology**

* Agile development with 2-week sprints
* Continuous integration and deployment
* Feature flags for gradual rollout
* A/B testing for UI components
* Automated testing for ML models

**Quality Assurance**

* Model validation and performance metrics
* User acceptance testing for AI features
* Performance testing under load
* Security testing for data protection
* Compliance verification for regulatory requirements

**Documentation**

* Technical documentation for AI components
* User guides for advanced features
* API documentation for integration
* Model cards for ML models
* Training materials for end users

[ISO 9001:2015](https://www.iso.org/standard/62085.html)

Quality management systems — Requirements

[Reference number](https://www.iso.org/standard/27001)

[ISO/IEC 27001:2022](https://www.iso.org/standard/27001)

[© ISO 2025](https://www.iso.org/standard/27001)

[Edition 3](https://www.iso.org/standard/27001)

[2022-10](https://www.iso.org/standard/27001)

[ISO/IEC 27001:2022](https://www.iso.org/standard/27001)

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

[Reference number](https://www.iso.org/standard/81230.html)

[ISO/IEC 42001:2023](https://www.iso.org/standard/81230.html)

[2023-12](https://www.iso.org/standard/81230.html)

[ISO/IEC 42001:2023](https://www.iso.org/standard/81230.html)

Information technology — Artificial intelligence — Management system

[ISO 45001:2018](https://www.iso.org/standard/63787.html)

Occupational health and safety management systems — Requirements with guidance for use

[ISO 14001:2015](https://www.iso.org/standard/60857.html)

Environmental management systems — Requirements with guidance for use

[ISO 26000:2010](https://www.iso.org/standard/42546.html)

Guidance on social responsibility

[ISO 50001:2018](https://www.iso.org/standard/69426.html)

Energy management systems — Requirements with guidance for use