

1. Introduction

Oyster is engineered as a secure, compliant, and highly integrated operational platform designed to support no matter the size to meet strict confidentiality, regulatory, and audit requirements. This document provides a detailed overview of Oyster's technical architecture, security controls, compliance capabilities, and integration options.

2. Hosting Environment & Infrastructure

2.1 Certified European Hosting

Oyster is hosted exclusively in European ISO/IEC 27001-certified data centres, ensuring alignment with GDPR and modern security standards. Key characteristics include:

- Redundant hosting across multiple EU locations
- Encrypted data storage
- Encrypted transport (TLS) for all connections
- Automated daily backups with multi-point restore capability
- Strict data-location guarantees within the EU

2.2 Platform Architecture

Oyster operates on a cloud-based, multi-tenant architecture designed for reliability and scalability.

The system supports:

- Multi-device access (desktop, laptop, tablet, mobile)
- Uniform security enforcement across all endpoints
- Session-based authentication
- Continuous monitoring of system health and uptime

3. Security Model

3.1 Access Control

Oyster uses a granular, role-based authorisation framework:

- User-specific permission sets
- Segregation of duties
- Compartmentalised data visibility
- Field-level protection for sensitive information
- Action-level restrictions (view, edit, approve, export)

This ensures users only access the information required for their role.

3.2 Monitoring & Audit Trails

Oyster provides:

- Real-time monitoring of access attempts
- Origin tracking (IP, device, timestamp)
- Revision-safe logs (in advanced packages)
- Full change history for audit and compliance inspections

3.3 Data Integrity Controls

- Automatic validation of critical fields
- Prevention of duplicate entries
- Controlled approval workflows
- Audit-ready reporting

4. eCompliance – Government-Certified Digital Reporting

4.1 Regulatory Coverage

Oyster supports the growing global requirement for certified digital invoice submission and real-time VAT reporting. Supported frameworks include:

- Italy SDI
- Portugal ATCUD / SAF-T
- Germany
- France eReporting - each company must have a valid SIREN registered in the French taxpayer directory before eInvoicing or eReporting can be activated.
- EU ViDA (2024–2028)
- Peppol BIS 3.0
- EN 16931 semantic model

4.2 Technical Workflow

When an invoice is issued:

- a. Oyster generates a structured XML/JSON file compliant with the relevant national standard.
- b. The invoice is transmitted securely to the government agency or Peppol Access Point.
- c. A human-readable PDF is produced with embedded certified coding.
- d. Submission logs and government responses are recorded.
- e. The invoice is archived in the secure hosted environment.

4.3 Security & Hosting

All eCompliance processing is executed within Oyster's certified European hosting environment, ensuring:

- Secure transmission
- Secure storage
- GDPR compliance
- Full audit traceability

5. eInvoicing – Certified Peppol & EN 16931 Infrastructure

5.1 Standards & Protocols

Oyster's eInvoicing module supports:

- EN 16931 semantic model
- Peppol BIS 3.0
- AS4 protocol for secure global transmission
- Certified Peppol Access Point connectivity
- Cross-border invoice interoperability

5.2 Processing Flow

- Invoice data is converted into EN 16931-compliant structure.
- Transmission occurs via AS4 to the Peppol network.
- Delivery receipts, acknowledgements, and error codes are managed automatically.
- No external apps or third-party systems are required.
- The process is fully integrated into the Pearl modules.

6. Languages & Internationalisation

Oyster is designed for multilingual, cross-border operations. The platform supports multiple languages across both the user interface and data outputs, enabling seamless use in international teams and multi-jurisdictional environments.

6.1 Multilingual UI

- Interface available in multiple languages
- Consistent terminology across modules
- Localised formatting for dates, numbers, currencies
- Language-specific validation rules where required (e.g., fiscal codes)

6.2 Multilingual Data Outputs

- Invoices, documents, and operational reports can be generated in the client's preferred language
- eInvoicing outputs (XML/JSON) follow international standards regardless of UI language
- PDF outputs support multilingual headers, footers, and item descriptions

6.3 Cross-Border Operational Support

- Oyster's multilingual capabilities ensure that:
- International teams can work in their native language
- Clients and suppliers receive documents in the correct language
- Compliance outputs remain standardised even when UI language changes

7. UI Design & User Experience

Oyster's interface is designed to be clean, consistent, and intuitive, reducing training time and improving operational efficiency.

7.1 Consistent Design System

- Unified design language across all Pearl modules
- Clear visual hierarchy
- Minimalist layout optimised for speed and clarity
- No visual noise or unnecessary animations

7.2 Operational Efficiency

- Fast navigation between modules
- Logical grouping of functions
- Reduced click-depth for high-frequency tasks
- Mobile-friendly layouts for on-the-go access

7.4 Accessibility & Usability

- High-contrast design for readability
- Clear iconography
- Predictable interaction patterns
- Designed for users with varying levels of technical experience

8. Databasing & Data Architecture

Oyster's databasing model is engineered for stability, integrity, and long-term scalability.

8.1 Structured Data Architecture

- Normalised database design
- Prevention of duplicate entries

- Referential integrity across modules
- Consistent field definitions across all Pearls

8.2 Performance & Reliability

- Optimised queries for high-speed data retrieval
- Efficient indexing for large datasets
- Scalable architecture capable of supporting growing operational volumes

8.3 Data Integrity Controls

- Automatic validation of critical fields
- Controlled workflows for approvals
- Revision-safe logs (advanced packages)
- Full audit trail for compliance inspections

8.4 Interoperability

- Database structure designed for API integration
- Supports JSON/XML payloads for external systems
- Compatible with accounting platforms such as Exact Multiverse and custom ERPs

9. Integration With External Accounting Platforms

9.1 Integration Capabilities

Oyster supports secure API-based integration with external accounting and ERP systems, including:

- Exact Multiverse
- Custom in-house platforms

9.2 Technical Integration Model

Oyster provides:

- Two-way API communication
- JSON/XML payload support
- Secure token-based authentication
- Endpoint-specific mapping
- Automated synchronisation schedules

9.3 Client-Hosted Server Option

For organisations preferring to host their own data:

- Oyster builds a secure API connection to the client's server.
- Pearl modules read/write through the API.
- Oyster maintains access only for connection integrity and updates.
- Monthly maintenance ensures stable communication.

Important: When data is hosted on the client's server, the client assumes responsibility for backups, security, and regulatory compliance.

10. Backup, Redundancy & Disaster Recovery

10.1 Backup Strategy

- Automated daily backups
- Multi-point restore capability
- Redundant storage across multiple EU locations
- Protection against human error and force majeure

10.2 Disaster Recovery

- Rapid restoration procedures

- Infrastructure redundancy
- Continuous monitoring
- Failover mechanisms for critical services

11. Compliance & Audit Readiness

11.1 Audit Trails

Oyster provides:

- Revision-safe logs
- Timestamped activity records
- User-specific change tracking
- Exportable audit reports (depending on package)

11.2 Compliance Alignment

Oyster supports compliance with:

- GDPR
- EN 16931
- Peppol BIS 3.0
- AS4
- National digital invoice mandates
- EU ViDA framework

12. Summary

Oyster delivers a secure, compliant, and highly integrated environment for operational data management, digital invoicing, and regulatory reporting. Its strengths include:

- Certified European hosting
- Granular access control
- Comprehensive monitoring and audit trails
- Fully integrated eCompliance and eInvoicing
- Secure API connectivity with Exact Multiverse and other platforms
- Automated backups and disaster recovery
- Full alignment with modern regulatory frameworks

Oyster is designed for organisations requiring high confidentiality, regulatory certainty, and seamless integration with existing financial systems.