ITO

TRUST WHITEPAPER · 2026

SECURITY · PRIVACY · COMPLIANCE · GOVERNANCE

Trust is engineered.

How ITO builds, operates and governs mission-critical software for governments, public safety and critical infrastructure.

ISO 9001 | ISO/IEC 27001 | ISO/IEC 27701 | ISO 30301 | Security clearance · Ministry of Security of BiH

IT Odjel Mostar d.o.o. · ito.dev/en/trust-center · security@ito.dev

EXECUTIVE SUMMARY

Software institutions can trust for years

Mission-critical software needs more than innovation. It needs security, transparency, accountability and long-term commitment.

ITO designs platforms for institutions where reliability, security, data protection and operational continuity are essential: ministries, police authorities, border and intelligence services, regulators, employment services and cities.

This whitepaper describes how we protect that trust. It covers our independently certified management systems, the security controls built into every platform, how institutions keep full ownership and control of their data, our architecture and secure development lifecycle, and the principles that govern our use of AI.

One principle runs through all of it: **institutions remain in control**. ITO engineers secure, auditable and interoperable technology. The institution defines who may access information, which workflows exist, how long data is kept and who makes decisions.

CONTENTS

4 × ISO
certified management systems, independently audited every year

Cleared
security clearance issued by the Ministry of Security of BiH

Client-owned
all operational data stays owned and controlled by the institution

01 · OUR TRUST MODEL

Six pillars of trust

01

Security by design

Security is part of the whole software lifecycle: architecture, development, deployment, monitoring and continuous improvement.

02

Privacy by design

Institutions stay in control of operational data. Our platforms support lawful, transparent and accountable processing.

03

Compliance

Our processes and technology practices follow international standards for quality, information security, privacy and information governance.

04

Interoperability

Secure, standardised interfaces to existing government systems, registries, sensors and infrastructure.

05

Auditability

Critical actions, user activity and administrative changes are recorded for accountability and traceability.

06

Responsible innovation

Technology supports human decisions, makes institutions more efficient and strengthens public trust.

Institution defines. Platform enables.

Legislation

The legal framework sets out the institution's authority and obligations.

→

Client institution

- Policies & procedures
- User roles & permissions
- Retention rules
- Approvals & operational decisions

→

ITO platform

- Security & audit
- Workflows & notifications
- Integrations & APIs
- Reporting

> ITO builds secure software. Each institution remains responsible for its operational rules, user permissions, data retention policies and lawful use of the system, and remains the owner and controller of its data, procedures and decisions.

02 · CERTIFICATIONS & STANDARDS

Independently verified

For us, compliance is not a one-time certificate. It is how software is developed, projects are managed and information is protected. Our four management systems are audited by independent certification bodies every year.

ISO 9001

QUALITY MANAGEMENT

Structured project delivery, customer satisfaction and continuous improvement, with quality management built into every stage of software development.

Verify with SGS ↗

ISO/IEC 27001

INFORMATION SECURITY MANAGEMENT

A framework for identifying, managing and continuously improving information-security risks across the whole organisation.

Verify with RIGCERT ↗

ISO/IEC 27701

PRIVACY INFORMATION MANAGEMENT

Extends our security framework with structured privacy governance and accountability for personal data.

Verify with RIGCERT ↗

ISO 30301

INFORMATION GOVERNANCE

Lifecycle management of organisational information and documentation, so that it stays accurate, accessible and properly governed.

Verify with RIGCERT ↗

Security clearance · Ministry of Security of Bosnia and Herzegovina

ITO holds a security clearance issued by the Ministry of Security of BiH and works with institutions in the police, border and intelligence sectors.

STANDARDS AND FRAMEWORKS WE FOLLOW

- OWASP Secure Coding Practices and OWASP Top 10
- Microsoft Secure Development Lifecycle
- NIST Cybersecurity Framework (aligned where applicable)
- Zero Trust principles and Privacy by Design
- REST API best practices, OpenAPI, OAuth2, JWT

CONTINUOUS IMPROVEMENT CYCLE

- Annual certification audits and management reviews
- Risk assessments and internal audits
- Corrective actions and process optimisation
- Security awareness and secure-engineering maturity

ON OUR ROADMAP

SOC 2 · ISO/IEC 42001 alignment · Secure software development certification

03 · SECURITY

Security built into every phase

We build software for governments, law enforcement and public institutions, where the confidentiality, integrity and availability of information are essential. Security is considered in every phase, from the initial architecture to long-term maintenance.

Confidentiality

Only authorised users with clearly defined responsibilities can access sensitive information, through RBAC, strong authentication and granular permissions.

Integrity

Audit mechanisms, validation controls and traceability protect operational data and digital evidence against unauthorised changes.

Availability

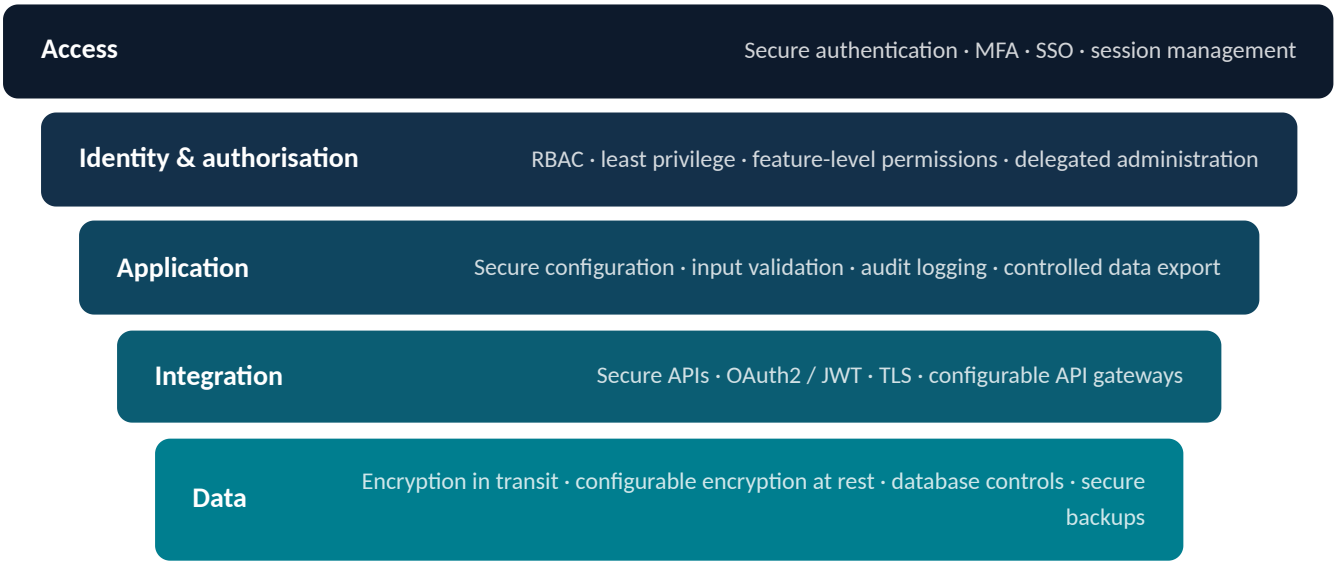
Redundancy, backups, disaster-recovery planning and high-availability deployments keep critical systems running when they are needed most.

Accountability

Every critical action can be attributed to an authenticated user, and comprehensive audit logs support governance and regulatory compliance.

Defence in depth

Public-sector systems need several layers of security, not a single protection mechanism. Our architecture combines complementary controls across user access, applications, integrations and data.



Identity & access management

- Microsoft Active Directory and LDAP integration
- Single sign-on and multi-factor authentication where required
- Organisational hierarchy and role-based permissions
- Delegated administration and granular, feature-level authorisation

Access rights are defined and maintained only by authorised personnel of the client institution.

Data protection

- TLS-encrypted communication and secure API authentication
- Database security controls and encryption of sensitive data
- Secure backup procedures and secure document storage
- Digital-evidence protection and controlled data export

Data ownership always stays with the client institution.

Audit & traceability

Complete visibility of administrative and operational activity supports accountability, forensic analysis and operational governance. We log:

- User authentication events
- Administrative and configuration changes
- Workflow actions and system events
- Evidence processing and the document lifecycle
- API interactions

Secure interoperability

Integrations must never weaken security. Our platforms connect to external systems through:

- REST APIs with OpenAPI specifications
- OAuth2 and JWT authentication
- TLS encryption end-to-end
- Configurable API gateways and secure service integrations

Security is a shared responsibility

ITO delivers secure, resilient and interoperable software. **Client institutions** define operational policies, user permissions, retention rules and lawful use of the system.

Responsible disclosure

Security enquiries, vulnerability reports and documentation requests: **security@ito.dev**

Secure by design · Defence in depth · Least privilege · Zero Trust principles · Privacy by design · Auditability · Secure integrations · Responsible disclosure · Continuous improvement

Privacy from the first line of architecture

Our software is designed for lawful processing, institutional governance and long-term protection of citizens' information. Privacy is considered from the earliest stages of system architecture, not added after development.

Data ownership

Institutions own their operational data. ITO processes information on their behalf, and ownership, governance and control stay with the institution.

Purpose limitation

Information is processed only for clearly defined institutional purposes, with no unnecessary processing.

Data minimisation

Systems process only what is needed for authorised tasks, and visibility can be tailored to each organisational role.

Transparency

Administrative actions are traceable and reviewable through audit records of critical events.

Accountability

Technology supports institutional accountability. It does not replace it.

Roles and responsibilities

CLIENT INSTITUTION	ITO
Data controller	Software development & maintenance
User management & access approvals	Security updates
Operational policies & internal governance	Technical support & documentation
Legal compliance & legal basis for processing	System integration
Data retention & authorisation procedures	Product quality & secure architecture

> The institution defines user roles, the organisational hierarchy, permissions, retention policies, the legal basis for processing, approval procedures, audit review policies and which integrations are authorised. ITO provides the platform that puts these rules into practice.

Privacy by design, in six principles

01
Data minimisation
Only the information required for operational purposes is processed.

02
Access limitation
Customer-defined permissions determine who sees what.

03
Separation of duties
Administrative responsibilities can be split across several roles.

04
Auditability
Critical actions remain traceable.

05
Secure communication
Data exchanged between systems is protected in transit.

06
Configurable retention
Retention periods follow applicable law and institutional policy.

Data lifecycle under institutional control

01	02	03	04	05	06	07
Collection	Validation	Processing	Storage	Operational use	Archiving	Deletion

Every stage follows policies defined by the institution. Our approach is guided by GDPR principles, Privacy by Design, ISO/IEC 27701, ISO/IEC 27001 and information-governance best practice.

Frequently asked questions

Who owns operational data?
The client institution. ITO does not acquire ownership of client operational data.

Can institutions configure retention policies?
Yes. Retention periods follow applicable legislation and internal governance policies.

Does ITO decide who can access information?
No. Permissions are defined and managed only by authorised personnel of the client institution.

Does ITO access operational data?
Only when the institution explicitly authorises it for maintenance, troubleshooting or support, and always under contractual obligations and security procedures.

05 · ARCHITECTURE

Modernise without replacing

Our architectures let institutions modernise their operations without replacing the systems they already have. Our engineering philosophy rests on openness, interoperability and long-term sustainability.

01

Modular by design

Independent functional modules, deployed as needed, working together as one integrated ecosystem.

02

Interoperability first

Designed to integrate securely with existing registries, databases, sensors and enterprise applications.

03

Vendor independence

Works with different hardware, operating systems and protocols, with no lock-in to a single vendor.

04

Scalability

Scales from a single department to nationwide deployment with the same security and governance model.

05

Security by architecture

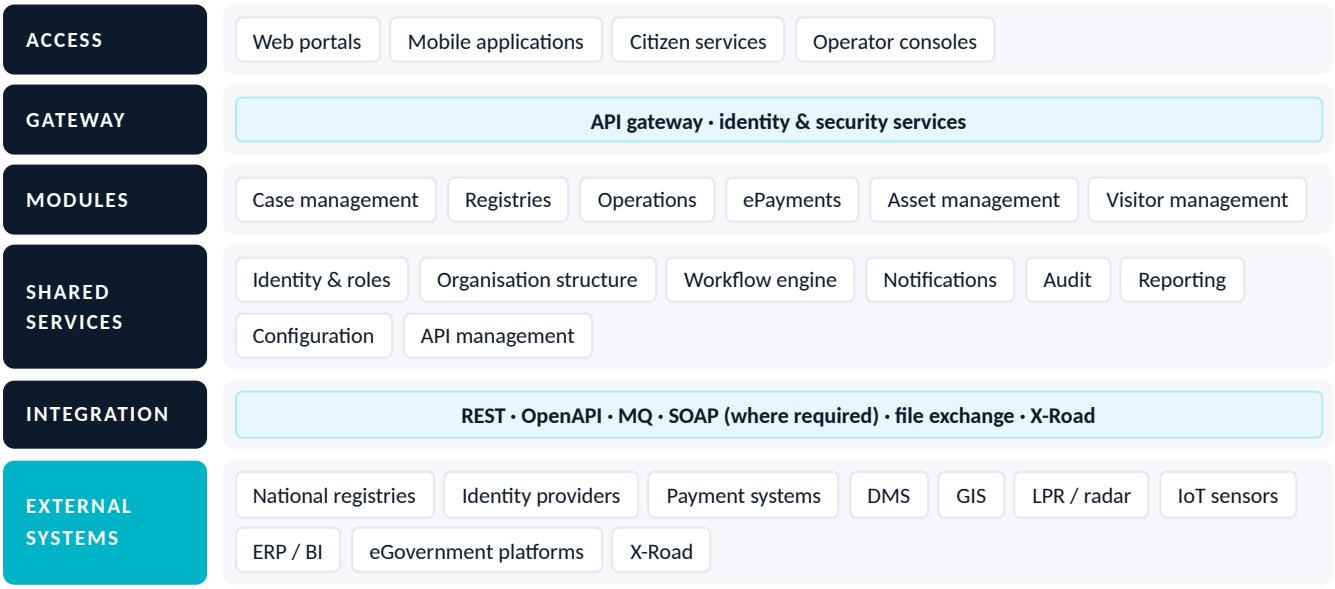
Identity, access control, secure APIs, encryption, auditability, monitoring and resilience are architectural decisions.

06

Operational resilience

High availability, backup and recovery, distributed deployment and offline capabilities where applicable.

Reference architecture



05 · ARCHITECTURE

Deployment models

Institutions choose the deployment model that fits their operational and regulatory requirements.

On-premises | Private cloud | Government cloud | Hybrid | Air-gapped environments | High-availability clusters | Disaster-recovery sites

Technology stack

BACKEND	.NET · ASP.NET Core · C#
FRONTEND	React · Flutter · Blazor
DATABASE	SQL Server · PostgreSQL · Elastic
MESSAGING	RabbitMQ · Azure Service Bus (if applicable)
MONITORING	Elastic · Kibana · Prometheus · Grafana
IDENTITY	Active Directory · LDAP · OAuth2 · JWT
API	REST · OpenAPI · Swagger
CONTAINERS	Docker

Performance & scalability

- Horizontal scaling and load balancing
- Caching and asynchronous processing
- Distributed services and background workers
- Event-driven processing

Data-flow principles

Information should move securely, and only when necessary.

- Minimal data movement
- Secure, encrypted integrations
- Institution-controlled governance
- Auditability and traceability

Long-term sustainability

- Open standards and vendor independence
- Backward compatibility and modular upgrades
- Configurable integrations
- Incremental digital transformation

We do not build projects. **We build platforms.**

We do not replace existing systems. **We integrate them.**

We do not lock customers into proprietary ecosystems. **We build interoperable architectures.**

We do not build software for today. **We engineer platforms that stay sustainable for the next decade.**

06 · SECURE DEVELOPMENT

Security is integrated, not added later

Every ITO solution is developed with a structured methodology that combines software architecture, security engineering, quality assurance and continuous improvement.

01	02	03	04	05	06	07	08	09
Business analysis	Solution architecture	Security review	Development	Code review	Testing	Deployment	Monitoring	Continuous improvement

Security review

Before implementation we evaluate authentication, authorisation, attack surface, data protection, auditability, integrations and risk.

Testing

Functional, regression, integration, performance and security testing, followed by user acceptance testing.

Controlled deployment

Deployment validation, configuration verification, migration checks, rollback planning and release documentation.

Development standards

Git-based version control, peer code review, CI/CD principles where applicable, secure coding, clean and layered architecture, and OWASP recommendations.

Change management

Every significant change goes through impact assessment, planning, implementation, testing, approval, deployment and review.

Secure supply chain

Trusted, supported suppliers and components, documented dependencies, vulnerability monitoring and update management.

DOCUMENTATION DELIVERED AS PART OF THE PRODUCT

- Business analysis and functional specification
- Architecture and API documentation
- Deployment guides and administration manuals
- User manuals, release notes and change logs

WHAT WE MEASURE

Code quality · Security findings · Test coverage · Release stability · Performance · Defect resolution time · Documentation completeness · Customer feedback

07 · RESPONSIBLE AI

AI that supports people, not replaces them

AI can improve operational efficiency, situational awareness and data analysis in public safety. It must always stay under human oversight and within the legal framework set by the competent institution.

01

Human oversight

People remain responsible for decisions. AI analyses, detects patterns and prioritises events.

02

Accountability

AI does not transfer legal responsibility from institutions to software.

03

Transparency

Users see what triggered a recommendation and what information was analysed.

04

Fairness

Model performance and relevance are continuously evaluated under institutional governance.

05

Security

AI services are protected by the same controls as the rest of the platform.

06

Continuous improvement

Models, datasets and behaviour are evaluated and improved throughout the lifecycle.

Technology may

- Analyse
- Correlate
- Recommend
- Prioritise
- Visualise

Technology should not independently

- Issue legal decisions
- Determine guilt
- Replace authorised officers
- Override institutional procedures

AI IN PRACTICE (RENATA)

Licence-plate recognition, vehicle classification, image enhancement, event prioritisation, anomaly detection and intelligent search. The aim is to reduce repetitive work, not to automate institutional decisions. AI features are **optional, configurable and can be disabled**.

EXPLAINABILITY

Recommendations come with supporting evidence, confidence indicators, linked operational data and traceable workflows.

GOVERNANCE

Institutions define the legal basis, operational policies, approval procedures, user permissions, deployment scope and acceptable use. Every AI capability is assessed for operational, security and privacy impact.

ALIGNED WITH

- EU AI Act
- OECD AI Principles
- ISO/IEC 42001
- NIST AI RMF
- Human-centric AI

Institutions remain in control

Technology should never determine institutional authority. Institutions determine authority, and technology enables it. Trust is created when technology, institutions and legal responsibilities are clearly separated.

Institutions determine

- Who may access information, and what is available
- Which workflows, approval chains and integrations exist
- How long information is retained, archived and deleted
- Organisational structure, audit policies and operational decisions

ITO is responsible for

- Software engineering and secure architecture
- Product maintenance, quality and security updates
- Interoperability and technical documentation
- Technical support

Data ownership

Operational information remains the property of the client institution. ITO does not acquire ownership of client operational data.

Open architecture

Open APIs, documented integrations and vendor independence mean clients never depend on our proprietary technology decisions.

Governance in practice

Clearly defined responsibilities, documented procedures, segregation of duties, controlled change management and continuous monitoring.

Principles we build by

- Technology should enable institutions, not replace them.
- Auditability strengthens accountability.
- Interoperability protects public investment.
- Transparency strengthens trust.
- Security protects public confidence.
- Innovation should always respect governance.

CITIZENS TRUST INSTITUTIONS. INSTITUTIONS TRUST TECHNOLOGY.

Technology must be worthy of that trust.

We are happy to share further security documentation, answer due-diligence questionnaires and walk your security team through any ITO platform.

SECURITY & DISCLOSURE	security@ito.dev
TRUST CENTER	ito.dev/en/trust-center
GENERAL ENQUIRIES	info@ito.ba · +387 36 830 003
COMPANY	IT Odjel Mostar d.o.o., Mostar, Bosnia and Herzegovina