

SECURITY ARCHITECTURE · ENGINEERING PRINCIPLES

Security is an engineering requirement.

Security architecture and engineering principles for mission-critical government software.

DOCUMENT ID	VERSION	CLASSIFICATION	DOCUMENT OWNER	REVIEW CYCLE	PUBLISHED
ITO-TRUST-SEC-001	1.0	PUBLIC	Information Security	Annual	October 2026

Security is not a feature. It is how we engineer.

Government institutions, public safety organisations and operators of critical services depend increasingly on digital platforms to support processes that require high levels of availability, integrity, confidentiality and accountability.

For ITO, security is therefore not an additional software feature. It is an **engineering requirement** that influences how systems are designed, developed, integrated, deployed and maintained throughout their lifecycle.

ITO develops software platforms for environments in which information may be operationally sensitive, access must be strictly controlled, system activities must be traceable and integrations frequently connect multiple institutional information systems and external data sources.

ITO platforms are designed to operate within institutional governance frameworks. The customer institution determines operational policies, authorised users, access rights, lawful purposes, retention requirements and other governance rules according to applicable legislation, internal procedures and contractual arrangements.

ITO provides the technology required to implement and enforce those rules within the scope of the deployed solution.

This whitepaper describes the engineering principles, processes and security controls that form the foundation of ITO software development and deployment. It is intended for technical decision-makers, information security professionals, public-sector organisations, partners and other stakeholders evaluating ITO technology.

OUR SECURITY APPROACH RESTS ON FOUR PRINCIPLES

01

Security by Design

Security requirements are considered during system architecture and development rather than introduced only after implementation.

02

Least Privilege

Users, services and system components should receive only the permissions required to perform their intended functions.

03

Defence in Depth

Security does not depend on a single control. Multiple technical and organisational safeguards are used across application, identity, data, integration and infrastructure layers.

04

Accountability and Traceability

Security-relevant activities should be recorded in a manner that enables institutions to understand how systems and information are being accessed and used.

CONTENTS

01	Executive summary	02
02	Security governance	04
03	Security risk management	05
04	Security by design	06
05	Identity & access management	08
06	Data security	10
07	API & integration security	12
08	Auditability & traceability	14
—	Architecture at a glance	15
09	Infrastructure & deployment	16
10	Secure development lifecycle	18
11	Vulnerability management	21
12	Operational security & incidents	22
13	Third-party & supply chain	24
14	Shared responsibility model	26
15	Business continuity & resilience	28
16	Standards & certifications	29
17	Security transparency	31
18	Vulnerability disclosure	32
19	Customer assurance	33
20	Conclusion	34

DOCUMENT CONTROL

DOCUMENT ID	ITO-TRUST-SEC-001
VERSION	1.0
CLASSIFICATION	PUBLIC
OWNER	Information Security
REVIEW CYCLE	Annual
PUBLISHED	October 2026

Institutions define the rules. ITO provides the technology.

ITO provides the technology required to implement and enforce institutional rules within the scope of the deployed solution. Security is shared between the technology provider, the customer institution, the infrastructure provider and, where applicable, third-party technology partners.



The full shared responsibility model is described in chapter 14. Governance rules are set by the customer institution according to applicable legislation, internal procedures and contractual arrangements. ITO platforms are designed to operate within those institutional governance frameworks.

THE INSTITUTION DETERMINES

- Operational policies
- Authorised users and access rights
- Lawful purposes of processing
- Retention requirements
- Other governance rules under applicable legislation and contracts

ITO PROVIDES

- Secure software architecture and engineering
- Technology to implement and enforce institutional rules
- Security controls within the scope of the deployed solution
- Maintenance and updates according to the agreed operational model

SCOPE OF THIS DOCUMENT



This document describes ITO's organisation-level security approach and common engineering principles.

Individual products and deployments may implement different security controls depending on their architecture, infrastructure, operational requirements and customer environment. Product-specific and deployment-specific security documentation may therefore complement this whitepaper.

Security as an organisational responsibility

Information security requires more than technical controls. It requires clearly defined responsibilities, documented processes, risk management, continuous improvement and organisational accountability.

ITO integrates information security into its management and engineering processes through policies, procedures and technical practices designed to protect the confidentiality, integrity and availability of information and systems.

SECURITY RESPONSIBILITIES ACROSS THE SOFTWARE LIFECYCLE

01	Solution architecture and design	02	Software development	03	Infrastructure and deployment
04	Access management	05	System integrations	06	Change management
07	Vulnerability management	08	Incident management	09	Backup and recovery
10	Supplier and technology risk	11	Continuous monitoring and improvement		

Security is treated as a **multidisciplinary responsibility** rather than an isolated activity performed exclusively by a security function.

Information Security Management

ITO maintains an Information Security Management System designed to provide a structured framework for managing information security risks. The framework supports systematic identification and treatment of risks associated with people, processes, technology and information.

ITO's information security management practices are supported by its ISO/IEC 27001 certification, alongside the other independently certified management systems listed below.

CURRENT CERTIFICATIONS

ISO 9001 QUALITY MANAGEMENT	ISO/IEC 27001 INFORMATION SECURITY MANAGEMENT	ISO/IEC 27701 PRIVACY INFORMATION MANAGEMENT	ISO 30301 INFORMATION GOVERNANCE
--------------------------------	--	---	-------------------------------------

 **Security clearance • Ministry of Security of Bosnia and Herzegovina**
ITO holds a security clearance issued by the Ministry of Security of BiH.

Controls proportionate to risk

ITO applies a risk-based approach to information security. Security requirements may differ significantly depending on the nature of a system, the information being processed, its users, deployment environment, integrations and operational purpose.

For this reason, security controls should be proportionate to identified risks rather than applied solely as a standard technical checklist.

SECURITY CONSIDERATIONS MAY INCLUDE

01

Data sensitivity

The nature and sensitivity of information processed by the system.

02

User population

Internal users, administrators, field personnel, citizens, external organisations or machine identities.

03

External exposure

Whether components are publicly accessible, institutionally restricted or deployed within isolated environments.

04

Integrations

Connections with government registers, identity systems, payment systems, sensors, cameras, third-party services or other external systems.

05

Operational criticality

Potential consequences of service interruption, data loss or unauthorised access.

06

Deployment environment

On-premises infrastructure, government or private cloud, hybrid architecture or other controlled environments.

07

Regulatory requirements

Applicable legislation, contractual requirements, institutional policies and sector-specific obligations.

HOW THE SECURITY ARCHITECTURE IS DETERMINED

ITO engineering requirements

Common security principles and engineering practices applied across ITO software development.

+

Implementation risk profile

The specific data, users, exposure, integrations, criticality, environment and regulatory context of each implementation.

→

Security architecture

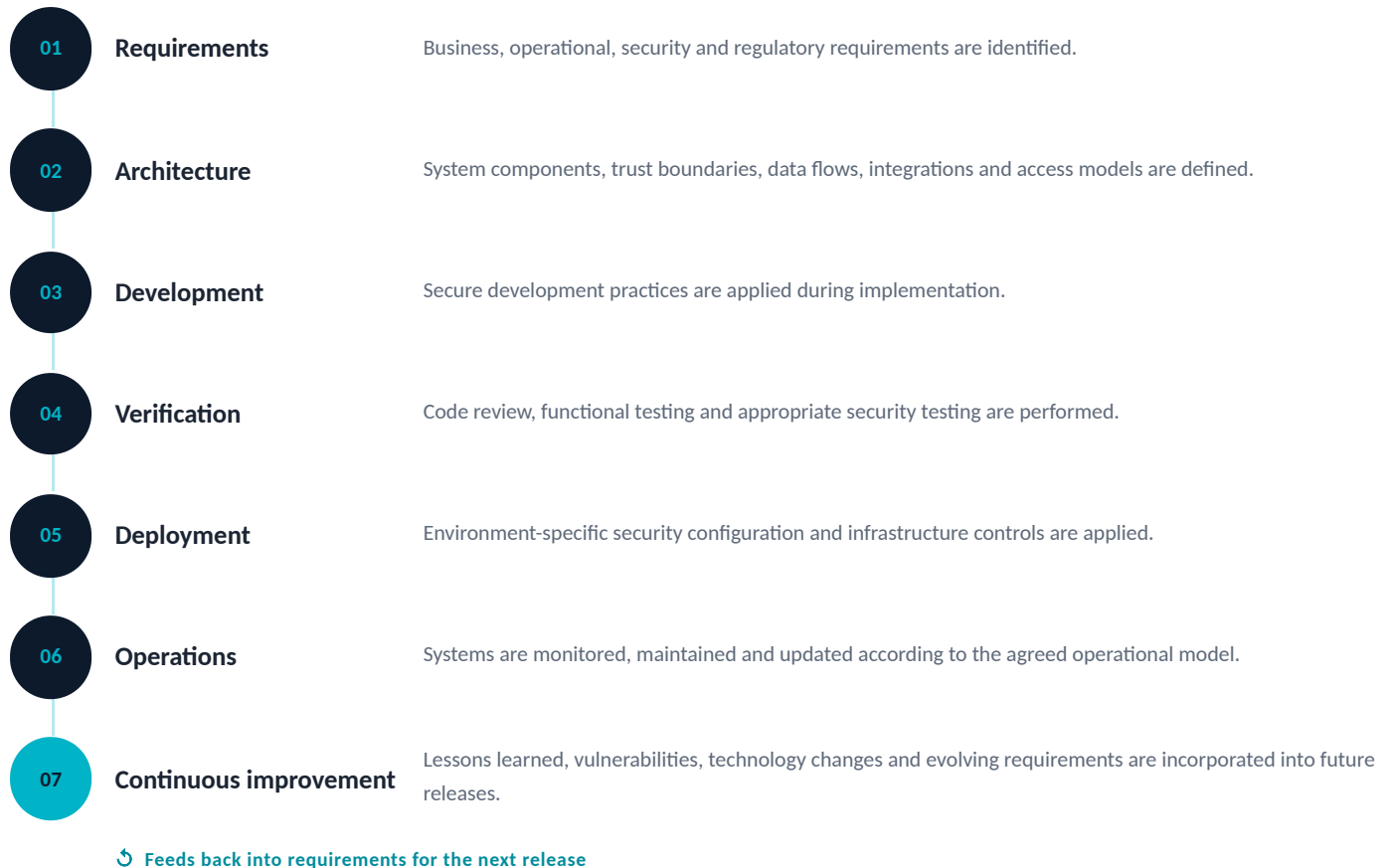
The resulting set of controls for that specific solution and deployment.

Security throughout the software lifecycle

Security considerations begin before development starts.

During solution design, engineering teams identify relevant information flows, users, integrations, trust boundaries and security requirements that may influence the architecture of the solution.

A TYPICAL LIFECYCLE



Security is part of every phase, from the identification of requirements to long-term operation, rather than a step introduced only after implementation.

Defence in depth and secure defaults

Defence in depth

ITO systems are designed around the principle that no individual security mechanism should represent the sole protection against a security threat.

Depending on the solution and deployment architecture, security controls may therefore exist across several layers.

A compromise or failure of one control should **not automatically result in unrestricted access** to the entire system.

Secure defaults

Where technically and operationally appropriate, ITO systems are designed so that security-sensitive functionality requires explicit configuration or authorisation rather than being unrestricted by default.

EXAMPLES MAY INCLUDE

- Restricted administrative functionality
- Role-based permissions
- Controlled system integrations
- Environment-specific configuration

SECURITY LAYERS

Users	ENTRY
Identity & Authentication	01
Authorisation & Access Control	02
Application Security	03
API & Integration Security	04
Data Protection	05
Audit & Monitoring	06
Infrastructure & Network Security	07
Operational Security	08

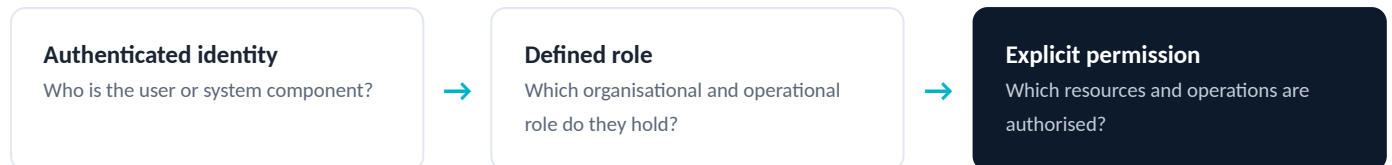
Detailed view. Layers shown are indicative; the controls implemented in each layer depend on the solution and its deployment architecture. A consolidated six-layer overview is shown in **Security architecture at a glance**.

Controlled access to systems and information

Identity and access management is a fundamental security layer across ITO platforms.

Access to system functionality and information is designed around **authenticated identities, defined roles and explicit permissions**. The objective is to ensure that users and system components can access only the resources required for their authorised responsibilities.

ITO solutions are designed to support access-control models appropriate to institutional organisational structures and operational requirements.



Role-Based Access Control

ITO platforms may implement Role-Based Access Control (RBAC) to associate permissions with defined organisational and operational roles.

DEPENDING ON THE SOLUTION, ACCESS POLICIES MAY CONSIDER



This allows customer institutions to translate organisational responsibilities into enforceable application-level permissions.

Principle of least privilege

ITO applies the principle of least privilege when designing access-control mechanisms.

Users, services and system components should receive **only the permissions necessary** to perform their intended functions.

Administrative and privileged functions should be separated from standard user operations wherever technically and operationally appropriate.

Authentication, privileged access and the access lifecycle

Authentication and enterprise identity

ITO solutions support integration with institutional identity-management infrastructure and standard authentication mechanisms.

SUPPORTED MECHANISMS INCLUDE

Active Directory / LDAP

Single Sign-On

Multi-factor authentication

Standards-based authentication and authorisation

All ITO platforms support these mechanisms. The model used in each deployment is selected according to the deployment environment and the customer's security requirements.

Administrative access

Administrative access represents a higher security risk and should therefore be subject to stronger controls.

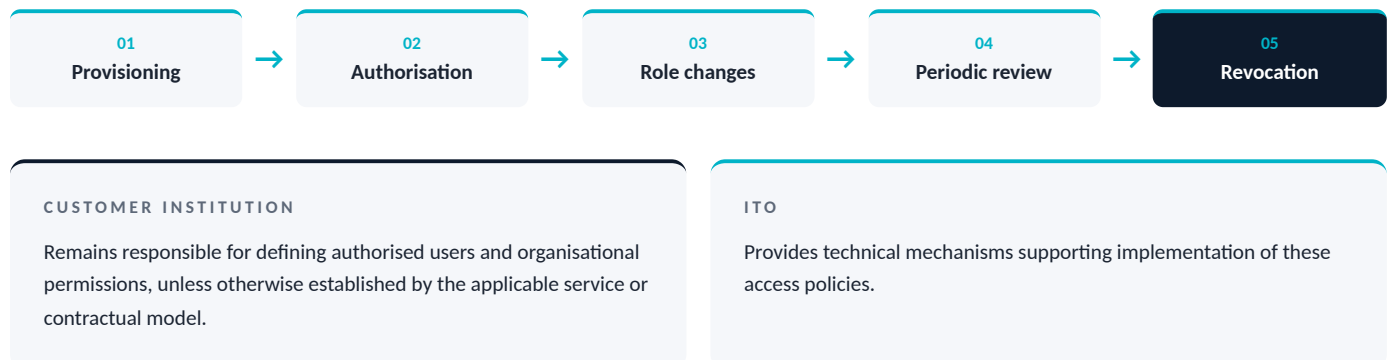
DEPENDING ON THE DEPLOYMENT MODEL, CONTROLS MAY INCLUDE

- Restricted administrative roles
- Separation of administrative responsibilities
- Stronger authentication requirements
- Controlled infrastructure access
- Logging of security-relevant administrative activities

ITO recommends that privileged access be limited to authorised personnel and periodically reviewed by the responsible organisation.

Access lifecycle

Access security does not end when an account is created. The identity lifecycle should address:



SUPPORTED ACROSS ALL ITO PLATFORMS

Enterprise identity, on every platform

✓ Active Directory / LDAP

✓ Single Sign-On

✓ Multi-factor authentication

✓ Local identity

✓ OAuth 2.0 / OpenID Connect

PLATFORMS

Renata

Carmen

AssetIX

eVa

CollaBIZ

eCTZen

GOV-cms

Marina

AURA

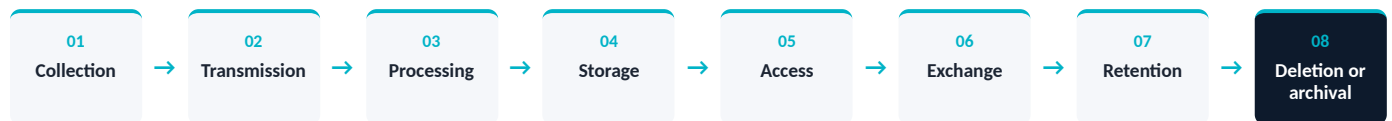
eAppointment

RIS WPR

Protecting information throughout its lifecycle

ITO systems may process information with different levels of sensitivity, ranging from administrative records to operational information used by government and public safety organisations.

Data protection must therefore be considered throughout the information lifecycle.



Security controls applied at each stage depend on the type of information, system architecture, deployment environment, customer requirements and applicable regulatory framework.

IN TRANSIT Data in transit

Communications between system components and external services should use secure transport mechanisms appropriate to the deployment architecture.

Where applicable, ITO solutions use industry-standard encrypted communication protocols such as **TLS** to protect information transmitted across networks.

Legacy or institution-specific integrations may require different mechanisms, which are assessed according to the requirements and capabilities of the connected system.

AT REST Data at rest

Protection of stored information may be implemented at different infrastructure and application layers depending on the deployed solution.

CONTROLS MAY INCLUDE

Database security mechanisms

Encrypted storage

Operating-system controls

Infrastructure-level encryption

Protected backup storage

The exact mechanisms depend on the customer infrastructure, database technology, deployment architecture and agreed security requirements.

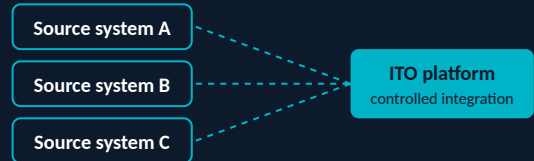
Minimisation, retention and recovery

Data minimisation

ITO supports the principle that systems should process information necessary for their defined operational purpose. System architecture should avoid unnecessary duplication, collection or retention of information where such processing is not required by operational, legal or technical requirements.

INTEGRATE WITHOUT CENTRALISING

Where possible, integrations can allow information to remain within **authoritative source systems** rather than requiring unnecessary replication into additional databases.



Data retention

Retention requirements are generally determined by applicable legislation, institutional procedures, operational requirements and contractual arrangements.

ITO PLATFORMS

May provide technical capabilities supporting retention and lifecycle policies.

RESPONSIBLE INSTITUTION

Determines the applicable rules within its legal and operational framework.

Backup and recovery

Backup and recovery requirements depend on the criticality of the solution and deployment architecture.

WHERE INCLUDED WITHIN THE AGREED SCOPE, BACKUP STRATEGIES MAY ADDRESS

Data integrity

Backup frequency

Retention

Access protection

Restoration procedures

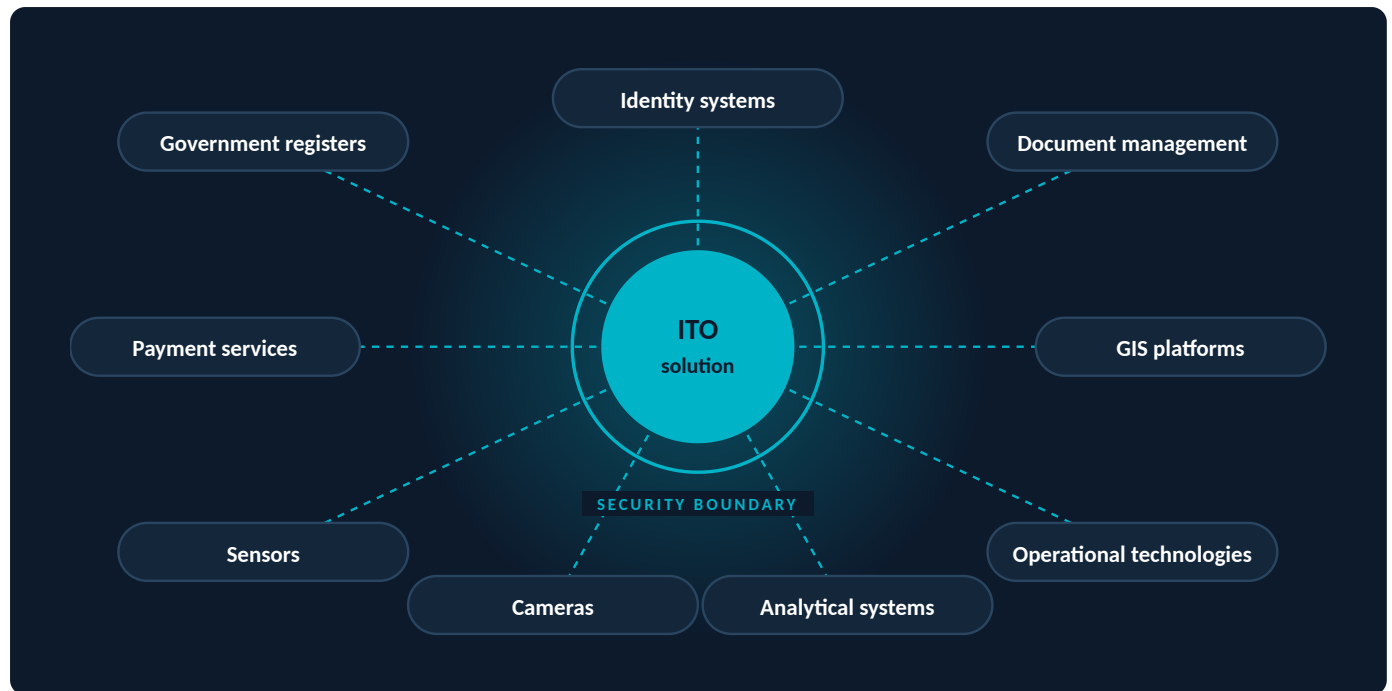
Recovery objectives

Backup mechanisms should be periodically verified through appropriate restoration or recovery testing.

Secure interoperability

Modern government platforms rarely operate independently. Every integration creates both operational value and a potential security boundary.

For this reason, interoperability must be engineered with security in mind.



Integration architecture

ITO favours controlled and documented interfaces between systems rather than uncontrolled direct access to underlying application databases. Where appropriate, integrations are implemented through APIs, web services, messaging infrastructure or other defined integration mechanisms.

AVOIDED

Uncontrolled direct database access

External systems reading or writing underlying application databases directly, without a defined interface.

FAVOURED

Controlled, documented interfaces

APIs, web services, messaging infrastructure or other defined integration mechanisms, providing clearer separation between systems.

APPLIED AT THE INTEGRATION BOUNDARY

Authentication

Authorisation

Validation

Logging

Lifecycle management

Protecting the integration boundary

API security

Depending on the integration architecture, API security controls may include:

01 Authenticated API access	02 Authorisation of API operations	03 TLS-protected communication
04 Token-based authentication	05 OAuth 2.0 or related standards, where applicable	06 Request validation
07 Controlled service accounts	08 Logging of relevant integration activity	09 Rate or access restrictions, where required

External systems

Security of an integration depends on both sides of the connection.

ITO may provide secure integration capabilities, but the overall security of an information exchange can also depend on the architecture, protocols and controls supported by the external system.

Where legacy systems or institution-specific technologies are involved, appropriate compensating controls may be required.

Integration credentials

Credentials, certificates, tokens and other secrets used for system-to-system communication should be protected against unauthorised access and unnecessary exposure.

Their storage, distribution, rotation and revocation should follow appropriate security procedures based on the deployed architecture.

Storage

Distribution

Rotation

Revocation

INTEROPERABILITY WITHOUT UNNECESSARY DATA DUPLICATION

Connect authoritative sources. Don't copy them.

ITO's integration philosophy is based on connecting authoritative information sources rather than automatically creating additional copies of institutional data.

Where operational and technical requirements permit, systems can retrieve or exchange required information through controlled integrations while authoritative data remains within the responsible source system. This can reduce unnecessary data duplication while supporting consistent access to current information.

Accountability through auditability

In mission-critical information systems, controlling access is only part of the security model. Institutions may also need to understand:

Who?

Who accessed the system?

What?

What action was performed?

When?

When did it occur?

Which?

What system or process was involved?

Auditability supports accountability, security investigations, operational oversight and compliance processes.

Audit logging

Depending on the product and deployment configuration, ITO solutions may record security-relevant and operational events such as:

- Authentication events
- User actions
- Administrative activities
- Changes to relevant records
- System integrations
- Selected data access events
- Workflow transitions
- System errors and security-relevant events

The exact scope of logging depends on system architecture, customer requirements and applicable governance policies.

Audit log protection

Audit information should itself be protected against unauthorised access, modification and deletion.

Access to audit information should therefore be limited according to appropriate administrative and security responsibilities.

Retention of audit records should be defined according to operational, contractual and applicable regulatory requirements.

Supporting institutional oversight

Audit capabilities can enable authorised institutional personnel to investigate activities, review system usage and reconstruct relevant sequences of events.

TECHNOLOGY PROVIDES

The evidence necessary for oversight.

THE INSTITUTION REMAINS RESPONSIBLE FOR

Defining governance procedures and determining how audit information is reviewed and acted upon.

Coordinated controls, end to end

A consolidated view of the controls described in chapters 4–8, grouping the detailed defence-in-depth layers of chapter 4.

INSTITUTIONAL GOVERNANCE

Policies • Roles • Procedures • Legal basis



01	Identity & access	Authentication • RBAC • Least privilege
02	Application security	Authorisation • Validation • Secure coding
03	Integration security	APIs • TLS • Authentication • Validation
04	Data security	Transmission • Storage • Backup • Lifecycle
05	Auditability & monitoring	Logging • Traceability • Oversight
06	Infrastructure & operations	Hardening • Networks • Monitoring • Recovery

Security is not a single product feature. It is a set of **coordinated controls** spanning governance, identity, applications, integrations, data and infrastructure.

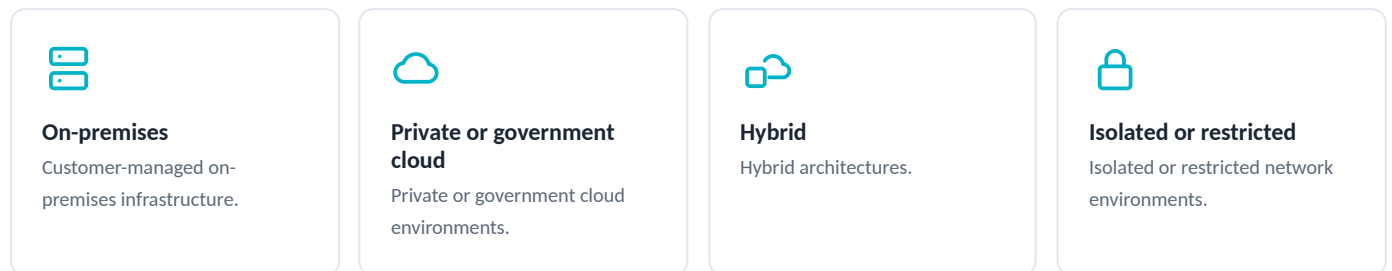
Security across deployment environments

Government and mission-critical systems may operate across different infrastructure models depending on institutional requirements, regulatory constraints, existing technology environments and operational needs.

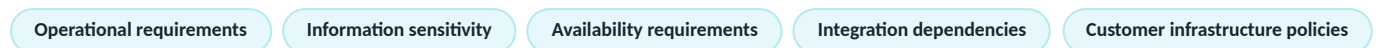
ITO solutions can be designed for deployment within customer-controlled infrastructure and other approved environments, subject to the architecture and requirements of the specific solution.

Security responsibilities therefore depend on the selected deployment and operational model.

DEPLOYMENT MODELS • DEPENDING ON THE PRODUCT AND PROJECT REQUIREMENTS



THE DEPLOYMENT MODEL IS SELECTED ACCORDING TO

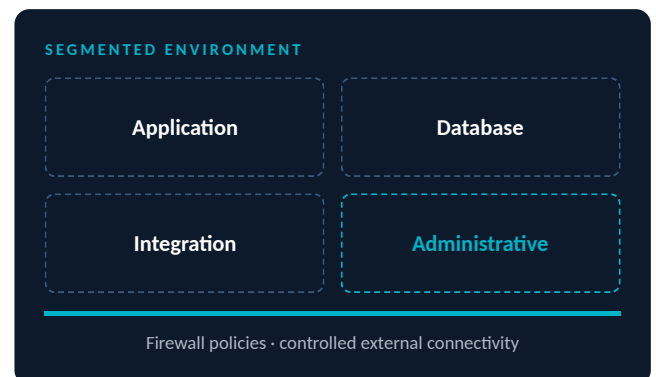


Network security

ITO solutions are designed to operate within appropriately segmented network environments.

DEPENDING ON THE DEPLOYMENT ARCHITECTURE, CONTROLS MAY INCLUDE

- Separation of application, database, integration and administrative components
- Firewall policies
- Restricted management interfaces
- Encrypted communications
- Controlled external connectivity
- Monitoring of relevant network activity



Network security is implemented jointly with the customer or infrastructure provider according to the agreed responsibility model.

Hardening, separation and resilience

System hardening

Production environments should be configured to minimise unnecessary services, interfaces and privileges.

HARDENING ACTIVITIES MAY INCLUDE

01

Secure operating-system configuration

02

Restricted administrative access

03

Removal or disabling of unnecessary services

04

Secure configuration of databases and application servers

05

Controlled network exposure

06

Management of default accounts and credentials

Deployment-specific hardening requirements may be documented as part of implementation and operational procedures.

Environment separation

Where applicable, development, testing and production environments should be logically or physically separated.

DEVELOPMENT

Broadest access

TESTING

Restricted access

PRODUCTION

Most restrictive access

Production information should not be introduced into development or testing environments unless there is a justified requirement and appropriate protection is applied.

Access to production environments should be more restrictive than access to development environments.

Availability and resilience

Availability requirements vary according to the operational criticality of each system. Where required by the solution architecture and contractual scope, ITO systems may support mechanisms such as:

Redundancy

High-availability configurations

Backup

Recovery procedures

Disaster-recovery architectures

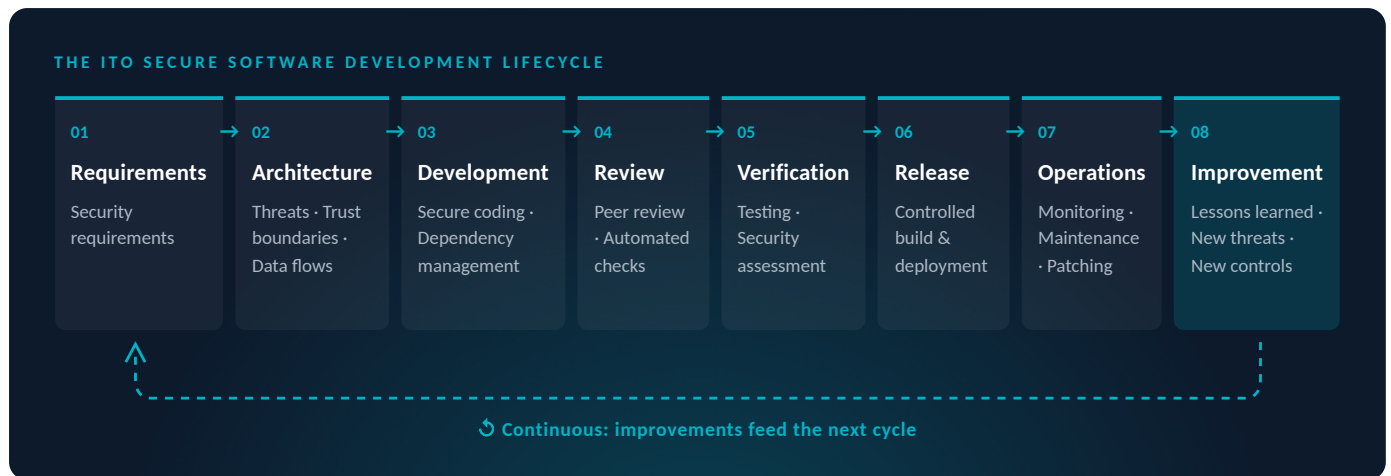
Recovery objectives and availability targets should be defined for each deployment according to customer requirements and the agreed service model.

Security is part of engineering

Security cannot be effectively introduced only at the end of software development.

ITO therefore integrates security considerations throughout the software lifecycle, from requirements and architecture to development, testing, deployment and maintenance.

The objective is to identify security requirements and potential risks as early as reasonably possible, when they can be addressed more effectively through architecture and design.



Security is a **lifecycle**,
not a release gate.

Requirements, architecture and secure development

10.1 Requirements

Security begins with understanding the system. During requirements analysis, relevant considerations may include:

- Types and sensitivity of information
- User groups and privileges
- External interfaces
- Authentication requirements
- Audit requirements
- Regulatory and contractual requirements
- Availability requirements
- Operational environment

For mission-critical systems, security requirements form part of the overall solution requirements rather than a separate post-development activity.

10.2 Architecture & design

Solution architecture establishes the security boundaries of the system. Architecture activities may therefore consider:

- Trust boundaries
- Identity flows
- Data flows
- External integrations
- Privileged operations
- Logging requirements
- Network boundaries
- Failure scenarios

Where appropriate, higher-risk functionality receives additional security consideration during design.

10.3 Secure development

ITO developers are expected to follow secure coding principles appropriate to the technologies and applications being developed.

DEVELOPMENT PRACTICES MAY INCLUDE

- 01 Input validation
- 02 Secure authentication and authorisation implementation
- 03 Appropriate error handling
- 04 Protection of sensitive information
- 05 Dependency management
- 06 Avoidance of known insecure development patterns

OWASP guidance may be used as a reference for relevant web and application-security risks.

Review, testing, release and maintenance

10.4 Code review

Code changes should be subject to appropriate review before being introduced into production releases.

REVIEW MECHANISMS MAY INCLUDE

Peer review

Pull-request workflows

Automated checks

Additional review for security-sensitive components

The level of review may depend on the risk and complexity of the change.

10.6 Release & deployment

Software releases should follow controlled processes that provide appropriate traceability between source code, build artefacts, configuration and deployed versions.

Source code



Build artefacts



Configuration



Deployed version

Production deployment should be limited to authorised personnel or automated deployment processes according to the applicable project model. Changes affecting security-sensitive functionality should receive appropriate review and testing before production deployment.

10.5 Security testing

Security verification may include a combination of automated and manual activities depending on system risk and project requirements. These may include:

01 Dependency and vulnerability scanning

02 Static analysis

03 Dynamic application testing

04 Manual security review

05 Penetration testing

06 Configuration review

07 Authentication and authorisation testing



Not every technique is necessarily applied to every release or product. Testing depth is determined according to risk, architecture, contractual requirements and release scope.

10.7 Maintenance

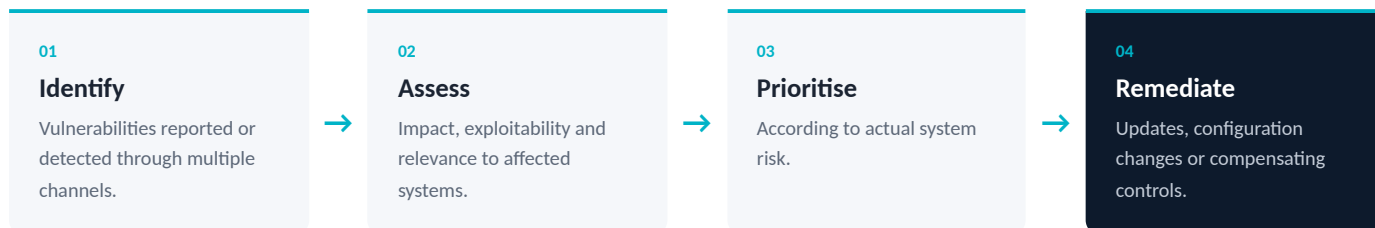
Security continues after deployment. ITO maintains software through controlled updates, corrective releases and security-related improvements according to applicable support and maintenance arrangements.

Newly identified vulnerabilities, technology changes and lessons learned may result in updates to applications, dependencies, configurations or engineering practices.

Identifying and managing security weaknesses

Software security evolves continuously. New vulnerabilities can emerge in operating systems, frameworks, libraries, infrastructure components and application code after a system has already been deployed.

ITO therefore treats vulnerability management as an ongoing component of software maintenance and security governance.



Vulnerability sources

Potential vulnerabilities may be identified through different channels, including:

- Internal testing
- Automated security tooling
- Software dependency advisories
- Technology vendors
- Customer reports
- External security assessments
- Responsible reports from independent security researchers

Identified vulnerabilities should be assessed according to their potential impact, exploitability and relevance to affected systems.

Dependency security

Modern software relies on third-party libraries, frameworks and infrastructure components.

ITO development teams should therefore maintain awareness of security vulnerabilities affecting relevant dependencies and assess updates where required.

Risk-based prioritisation

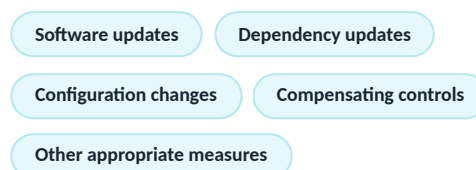
Not every published vulnerability represents the same level of risk to every deployed system. Assessment should consider factors including:



This enables remediation activities to be prioritised according to actual system risk.

Remediation

Where a vulnerability affecting an ITO-maintained component is confirmed, remediation may include:



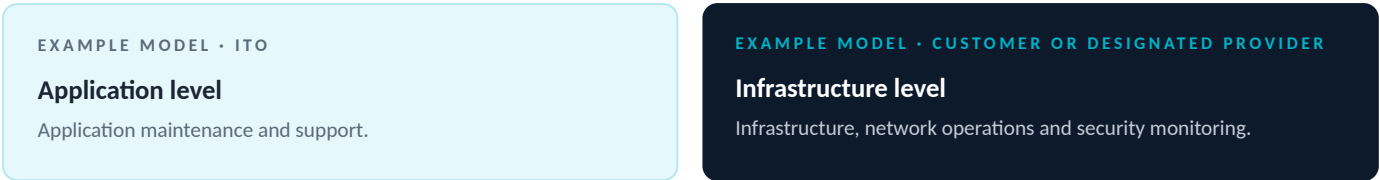
Remediation priority should reflect the assessed security risk and operational context.

Security continues after deployment

Deployment does not represent the end of the security lifecycle. Mission-critical systems require ongoing maintenance, monitoring, controlled changes and clearly defined procedures for responding to operational and security events.

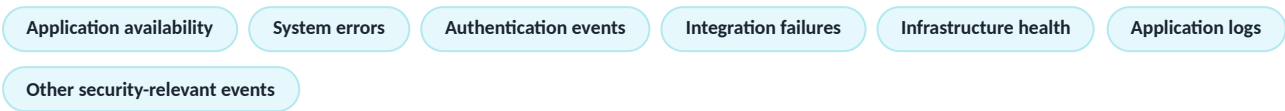
The exact operational model depends on the deployment architecture and contractual arrangement. In some environments, ITO may provide application-level maintenance and support while infrastructure, network operations and security monitoring remain under the control of the customer institution or its designated infrastructure provider.

For this reason, operational security responsibilities should be clearly defined for each deployment.



Security monitoring

Depending on the solution and agreed operational model, monitoring may include:

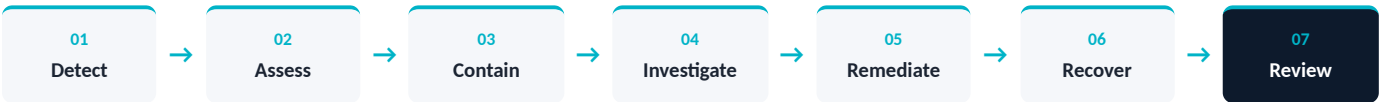


Where ITO does not operate the underlying infrastructure, relevant monitoring responsibilities may remain with the customer institution or its designated service provider.

Incident management

Security incidents require coordinated technical and organisational response. ITO's incident-management approach should support the identification, assessment, containment, remediation and review of security incidents affecting systems or services within ITO's area of responsibility.

A TYPICAL INCIDENT LIFECYCLE

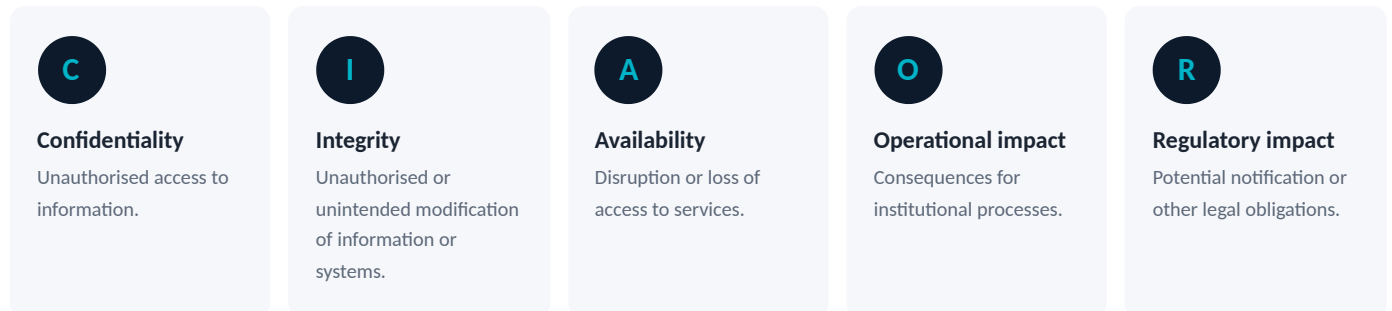


Where an incident involves customer-controlled infrastructure, institutional data or third-party systems, response activities should be coordinated with the responsible organisation according to established communication and escalation procedures.

Classification, communication and learning

Incident classification

Security events should be assessed according to their potential impact on:



Incident communication

Where a confirmed incident affects a customer environment within ITO's responsibility, communication should follow the applicable contractual, legal and operational requirements.

ITO and the customer institution should maintain appropriate escalation channels for security-relevant events.

Lessons learned

Significant security incidents should contribute to continuous improvement. Post-incident review may identify opportunities to improve:



SECURITY MATURITY

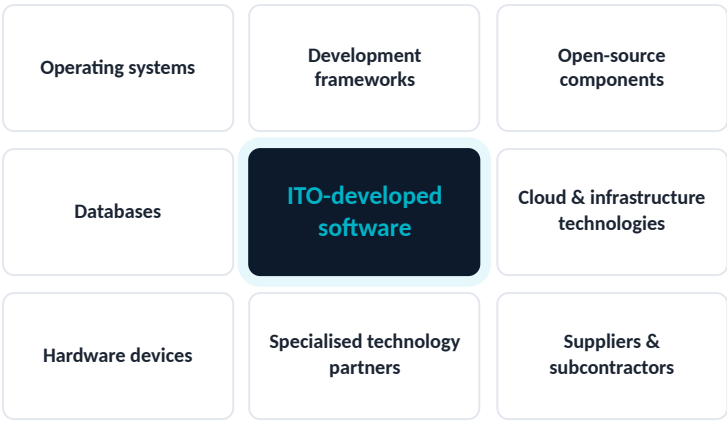
Security maturity is not the absence of incidents.

It is the ability to **prevent** where possible, **detect** effectively, **respond** appropriately and continuously **improve**.

Security extends beyond ITO

The security of a solution depends not only on software developed directly by ITO but also on the technologies and suppliers forming part of the overall system.

ITO recognises software and technology supply-chain security as part of its broader security responsibility.



A MODERN TECHNOLOGY ECOSYSTEM

Modern software platforms depend on technology ecosystems that may include operating systems, development frameworks, open-source components, databases, cloud or infrastructure technologies, hardware devices and specialised technology partners.

Third-party components

Third-party software components should be selected and maintained with consideration for:

- Security
- Technical maturity
- Support lifecycle
- Compatibility
- Operational requirements

Where vulnerabilities affecting relevant third-party components are identified, their applicability and potential impact should be assessed as part of vulnerability-management activities.

Open-source software

Open-source software can provide significant engineering and interoperability benefits but requires appropriate governance.

ITO should maintain visibility over security-relevant third-party dependencies used within its software and evaluate identified vulnerabilities and updates according to their relevance and risk.

Technology partners and supplier risk

Technology partners

ITO solutions may integrate technologies from specialised third-party vendors where these technologies provide capabilities required by a project. Examples can include:

Identity infrastructure	Databases	Cloud technologies	Document scanners	Cameras
LPR / ANPR devices	Biometric devices	Payment infrastructure	Other specialised systems	

The inclusion of a third-party technology does **not automatically imply** that ITO controls the security lifecycle of that technology.

Responsibilities should therefore be defined according to the specific integration and contractual model.

Supplier risk

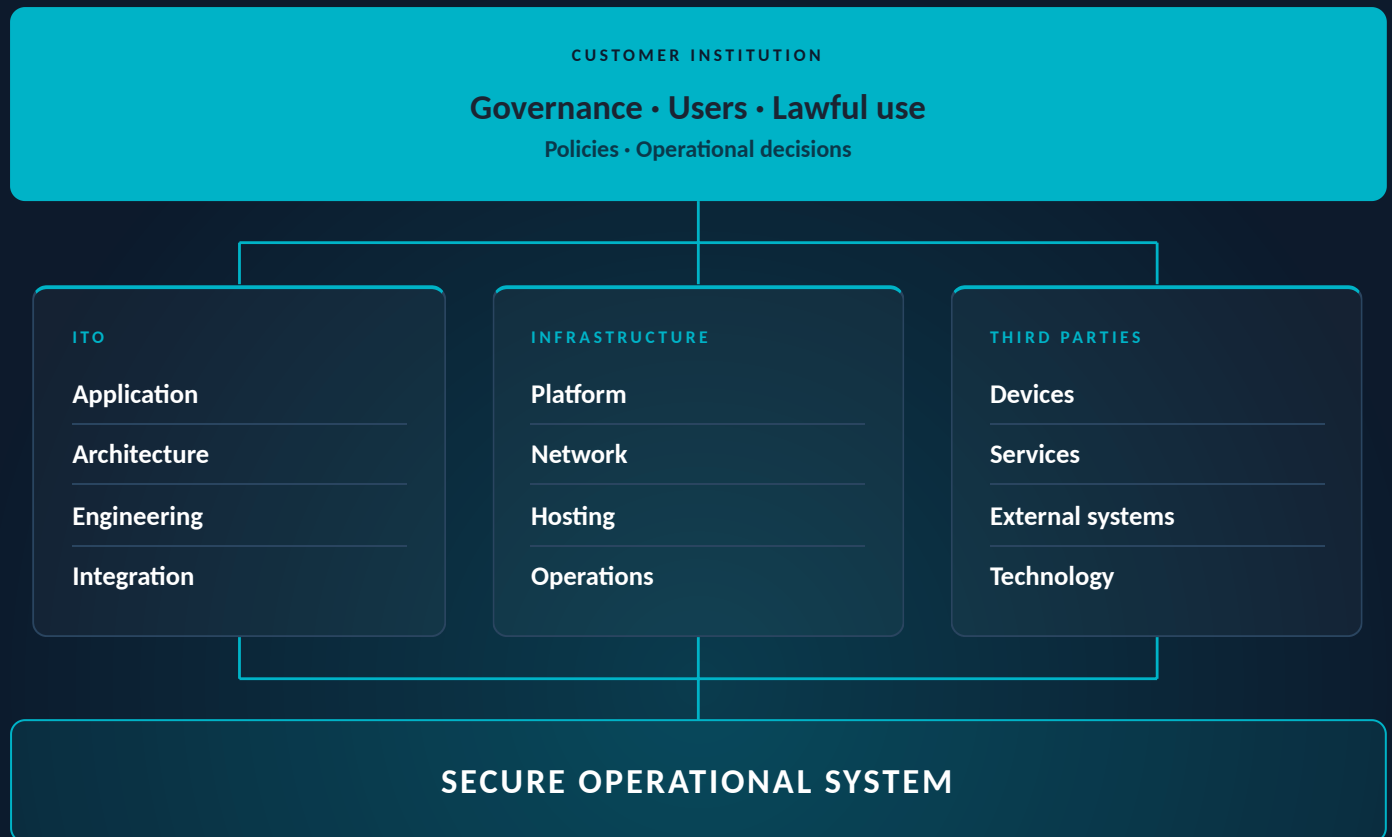
Where suppliers or subcontractors may have access to sensitive systems, information or development processes, security considerations should form part of supplier selection and management.

DEPENDING ON THE NATURE OF THE RELATIONSHIP, CONTROLS MAY INCLUDE

01 Contractual security requirements	02 Confidentiality obligations	03 Access restrictions	04 Review of relevant security capabilities
--------------------------------------	--------------------------------	------------------------	---

Security is a shared responsibility

The security of a mission-critical information system cannot be provided by software alone. Effective security depends on coordinated responsibilities across the technology provider, customer institution, infrastructure operators, users and third-party technology providers.



Technology provides **controls**. Institutions provide **authority and governance**.
Security depends on both.

Who is responsible for what

ITO promotes a shared-responsibility approach in which responsibilities are defined according to the architecture, deployment model, applicable legislation and contractual arrangement.



The precise allocation of responsibilities depends on the specific project and is defined according to its architecture, deployment model and contractual arrangement.

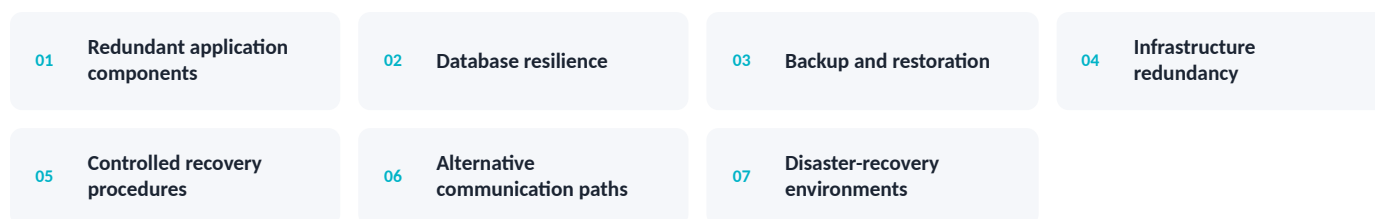
Designing for operational continuity

For mission-critical systems, security includes the ability to maintain or restore essential services following technical failure, infrastructure disruption, cyber incidents or other unexpected events.

Business continuity and disaster recovery requirements should therefore be defined according to the operational criticality of each deployment.

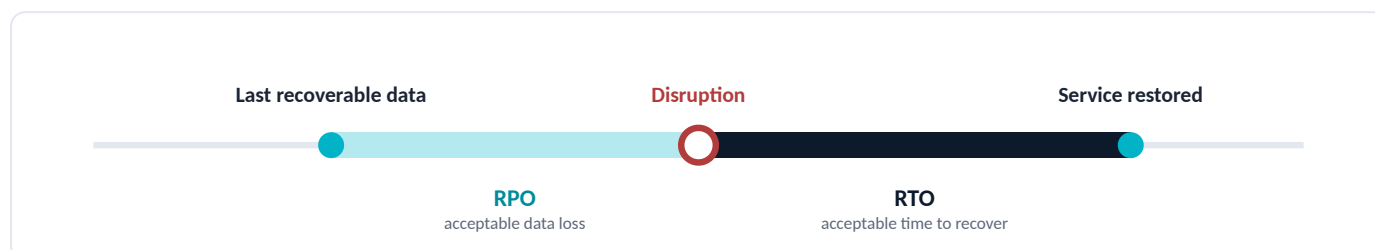
Resilience by architecture

Depending on project requirements, resilience mechanisms may include:



Recovery objectives

Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) should be defined according to customer requirements and the architecture of the specific deployment.



ITO does not apply a single universal recovery objective to all systems, because operational requirements differ significantly between solutions and institutions.

Recovery testing

Backup and disaster-recovery capabilities provide value only if they can be successfully used when required. Where recovery activities fall within ITO's operational scope, appropriate recovery procedures should therefore be documented and periodically verified.

Security supported by recognised standards

ITO uses internationally recognised management and engineering standards to provide structure, consistency and continuous improvement across its operations.

Certifications and external standards **complement, but do not replace**, technical security controls. Their purpose is to establish repeatable organisational processes for managing information security, privacy, quality and information throughout the lifecycle of ITO solutions.

CERTIFIED MANAGEMENT SYSTEMS

ISO/IEC 27001

INFORMATION SECURITY MANAGEMENT

ITO operates an Information Security Management System certified to ISO/IEC 27001. The ISMS provides a structured framework for identifying information-security risks, selecting appropriate controls, defining responsibilities and continuously improving security management practices.

ISO/IEC 27701

PRIVACY INFORMATION MANAGEMENT

ITO's privacy-management framework is supported by ISO/IEC 27701 certification. The standard extends information-security management with controls relevant to privacy information management and supports a systematic approach to managing privacy-related responsibilities.

ISO 9001

QUALITY MANAGEMENT

Quality management provides the organisational framework for consistent engineering, delivery and continuous improvement. Within ITO, quality and security are complementary disciplines: reliable software requires controlled engineering processes as well as appropriate technical safeguards.

ISO 30301

MANAGEMENT SYSTEMS FOR RECORDS

Where applicable to ITO's certified scope, records-management principles support controlled creation, management, retention and governance of organisational records.

This certification relates to ITO's organisational management system. It does not by itself certify records-management functionality of ITO products.

Engineering and security references

In addition to certified management systems, ITO engineering practices may reference established industry guidance and standards appropriate to individual technologies and projects.

These may include relevant guidance from:

OWASP
Application security

NIST
Cybersecurity and risk-management concepts

OpenAPI
Documented application interfaces

OAuth 2.0 / OpenID Connect
Where applicable to identity and API architectures

Privacy by Design
Principles for systems processing personal information

HOW TO READ ITO'S STANDARDS CLAIMS

CERTIFIED Management systems independently audited by an external certification body.	ALIGNED Practices designed to follow a framework's requirements, without a certification claim.	REFERENCED Industry guidance used where relevant to individual technologies and projects.
---	---	---

This whitepaper uses these terms deliberately and does not group them together.

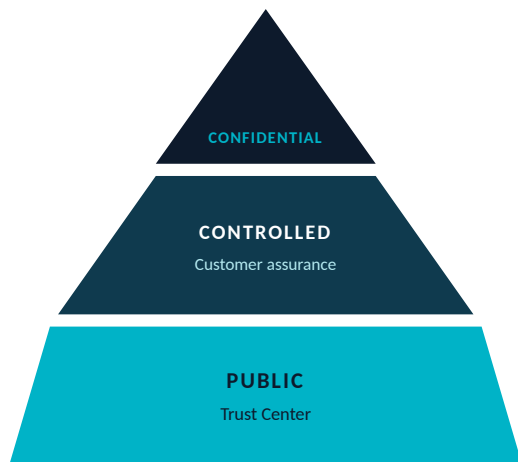
	CERTIFIED	REFERENCED
WHAT IT MEANS	Independently audited management system	Guidance used where relevant
APPLIES TO	ITO's organisation within the certified scope	Individual technologies and projects
IN THIS DOCUMENT	ISO/IEC 27001 • ISO/IEC 27701 • ISO 9001 • ISO 30301	OWASP • NIST • OpenAPI • OAuth 2.0 / OIDC • Privacy by Design

A reference to an industry framework indicates that its guidance informs ITO engineering practice. It is not a claim of certification against that framework.

Trust requires verifiable information

Security requires confidentiality, but security governance should not depend on secrecy.

ITO aims to provide customers and partners with sufficient information to understand how security is approached across its organisation, engineering processes and technology platforms, while protecting information that could create unnecessary security risk if disclosed publicly. Our transparency model therefore distinguishes between public, controlled and confidential security information.



● Confidential

Detailed security evidence. Available only where justified and subject to appropriate confidentiality arrangements.

● Controlled

Customer assurance. Available to qualified customers, partners or procurement processes where appropriate.

● Public

Available to everyone through the ITO Trust Center.

PUBLIC

- Security Whitepaper
- Privacy & Data Governance documentation
- Responsible AI Principles
- Secure Development overview
- Certification information
- Responsible Vulnerability Disclosure Policy
- High-level architecture documentation

CONTROLLED

- Detailed security questionnaires
- Security control matrices
- Product-specific security documentation
- Deployment architecture information
- Business continuity information
- Selected assessment summaries
- Data-flow documentation

CONFIDENTIAL

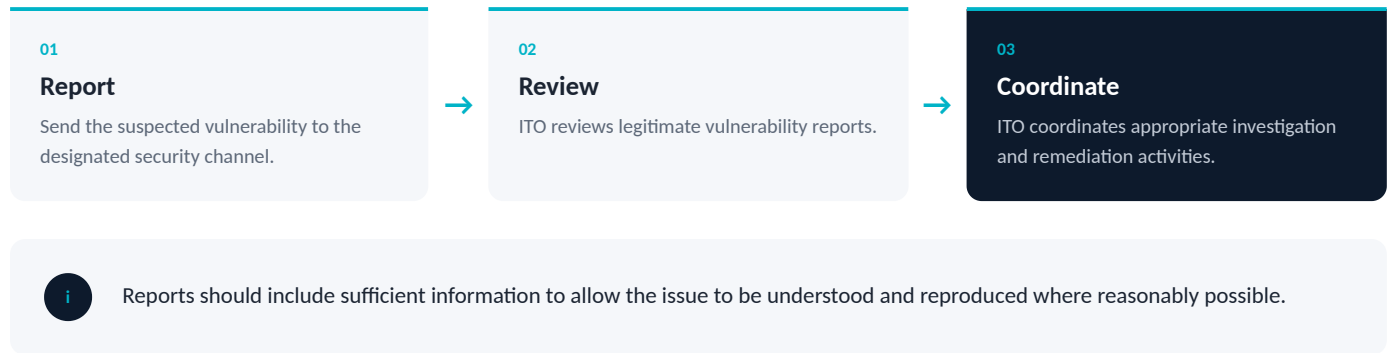
- Detailed penetration-test results
- Sensitive architecture information
- Internal security procedures
- Detailed vulnerability information
- Security configurations
- Incident-response details
- Other information that could materially increase security risk if publicly disclosed

Transparency does not require exposing sensitive security information. It requires providing the right evidence to the right stakeholders.

Working with the security community

ITO recognises that independent security researchers can contribute to improving the security of digital products and services.

We encourage responsible reporting of suspected security vulnerabilities affecting ITO products, services or publicly accessible infrastructure.



REPORTING CHANNEL

Found a potential vulnerability? Tell us.

ITO welcomes responsible reporting of potential security vulnerabilities affecting its products and publicly accessible systems.

Security researchers and other parties who believe they have identified a potential vulnerability are encouraged to contact the ITO security team through the designated security channel.

DESIGNATED SECURITY CHANNEL

security@ito.dev

TRUST CENTER

ito.dev/en/trust-center

Supporting security due diligence

Government institutions and enterprise customers may require additional security information during procurement, implementation or periodic supplier assessment.

ITO supports appropriate customer security-assurance processes by providing relevant technical and organisational documentation according to the nature of the project and sensitivity of the requested information.

DEPENDING ON THE ENGAGEMENT, THIS MAY INCLUDE

01 Security questionnaires	02 Certification evidence	03 Product-security documentation
04 Architecture documentation	05 Integration-security information	06 Deployment requirements
07 Access-control documentation	08 Data-flow information	09 Continuity and recovery information
10 Vulnerability-management information	11 Relevant independent assessment evidence	

Sensitive documentation may require appropriate confidentiality arrangements.

Product-specific security documentation

This whitepaper describes ITO's organisation-level security approach. Individual ITO platforms may have additional product-specific documentation addressing their architecture, security controls, integrations, deployment models and operational requirements.

PRODUCT SECURITY

RENATA Security & Trust Documentation

Product-specific security information for the RENATA law-enforcement platform is available on request through appropriate customer-assurance channels.

Available on request
security@ito.dev

Engineering trust

Security in mission-critical software cannot depend on a single technology, certification or control.

It requires disciplined engineering, clearly defined responsibilities, secure architecture, controlled development processes, operational awareness and continuous improvement.

ITO approaches security as a lifecycle extending from the first system requirement through architecture, development, deployment, operation and long-term maintenance.

NOT SIMPLY

To build software that performs its intended function:

OUR OBJECTIVE

To engineer digital platforms that institutions can **operate securely**, **govern responsibly** and **evolve over time**.

Trust is not added after software is built.
Trust is engineered into the way software is designed, developed and operated.



OUR COMMITMENT

Engineering Digital Trust.



SECURITY BY DESIGN • LEAST PRIVILEGE • DEFENCE IN DEPTH • ACCOUNTABILITY

Engineering Digital Trust.

Product-specific and deployment-specific security documentation may complement this whitepaper. We are happy to support your security team's due diligence for 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

DOCUMENT

ITO-TRUST-SEC-001 • Version 1.0 • PUBLIC • October 2026