DirSys

DirSys Whitepaper

Operationalising DORA with DirSys

A rule-driven model for digital operational resilience, ICT risk governance and continuous compliance

DirSys turns DORA from a static compliance checklist into a continuous, object-based governance process for digital operational resilience.

DirSys

Executive summary

The Digital Operational Resilience Act, DORA, requires financial entities to manage ICT risk in a structured, continuous and evidence-based manner. It introduces requirements for ICT risk management, ICT-related incident reporting, digital operational resilience testing and ICT third-party risk management.

For many organisations, the main challenge is not only to document compliance, but to operationalise DORA as part of day-to-day governance. This means being able to identify critical or important functions, understand which ICT services and suppliers support them, assess related risks, follow up controls, collect evidence and report status to management, auditors and supervisory authorities.

DirSys is well suited to support this type of operating model because its core structure is not based on static checklists. Instead, DirSys combines information objects, object properties, Security Spaces, a rule engine, control plans, risks, actions, evidence and Insights reporting.

This makes it possible to translate DORA from a regulatory framework into a practical governance model. Relevant controls, risks and actions can be activated based on the actual characteristics of the organisation’s business processes, ICT services, systems, suppliers and organisational units.

A key design principle is that DirSys Security Space does not store business information. Instead, Security Space acts as a secure grouping, access-control and context mechanism. It can be used to group the objects that together support a business area, critical or important function, process, ICT service or operational domain.

The detailed information remains on the relevant information objects and in the associated control plans. Business properties, classifications, ICT service attributes and supplier information are stored on the objects they describe. Control status, evidence and follow-up are managed in control plans. This avoids duplication, improves traceability and ensures that DORA-related information remains close to the business objects it governs.

By combining object-based governance, rule-driven control activation, evidence management and reporting, DirSys can help organisations manage DORA as a continuous operational process rather than as a separate spreadsheet, static checklist or one-off compliance project.

1 DORA as an operational governance challenge

DORA is not primarily a documentation requirement. It is a requirement to demonstrate that an organisation can identify, manage, monitor and test its digital operational resilience over time.

The practical challenge for organisations is therefore to answer questions such as:

- Which business functions are critical or important?
- Which ICT systems and services support them?
- Which suppliers are involved?
- Which risks exist?
- Which controls are in place?
- Which controls have been tested?
- Which gaps remain?
- Who is responsible?
- What evidence exists?
- What should be reported to management, auditors or supervisors?

DirSys can support this by turning DORA into a continuous control and governance process rather than a one-off compliance project.

DirSys is built around information objects, Security Spaces, frameworks, control plans, risks, actions and reporting.

The existing DirSys whitepaper defines an information object as information compiled for a specific purpose, for example a system, process or information set. It also describes Security Space as a protected space in which the assets to be protected, such as IT systems, are placed.

DirSys component	Role in DORA
Information objects	Describe processes, systems, services, organisational units and information assets
Object properties	Provide the facts used by the rule engine
Security Space	Groups objects and controls access through groups and roles
Rule engine	Determines which controls, risks and actions are relevant
Framework	Contains DORA, NIS2, ISO, GDPR or custom control structures
Control plans	Store control questions, status, evidence and follow-up
Risks	Capture exposure created by missing or weak controls
Actions	Turn gaps into accountable remediation work
Insights	Provides dashboards, reports and management views

This is central to DORA, because DORA controls should not apply equally to every object. A cloud-based system supporting a critical payment process should trigger a different control plan than a low-risk internal support tool.

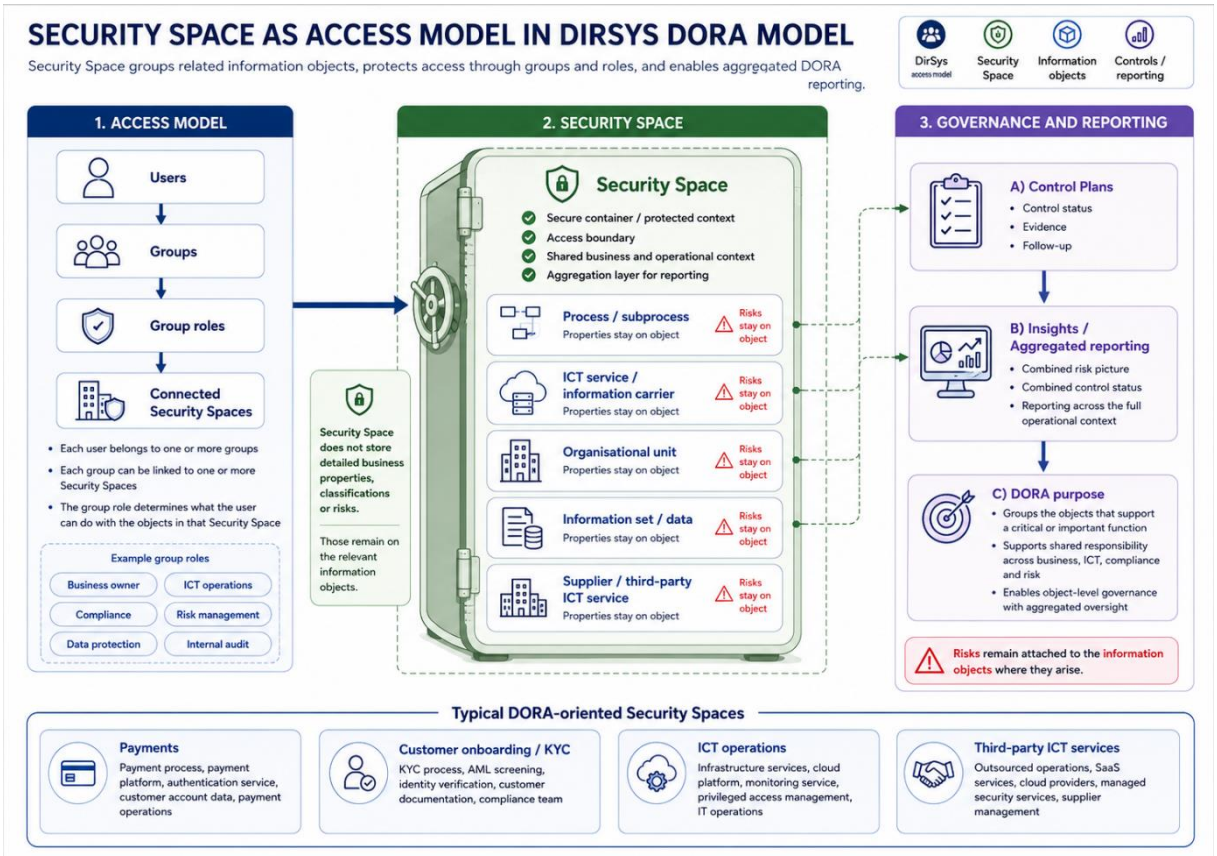
2 Security Space

In DirSys, a Security Space should be understood as a secure container — a “vault” — used to group, protect and provide controlled access to one or more information objects. It is a central part of the DirSys object-oriented model and provides a shared context for objects that belong together from a business, operational, security or compliance perspective.

A Security Space can include different types of information objects, such as ICT services, processes, subprocesses, organisational units, information carriers, information sets or other relevant object types. It can also include a combination of several object types that together represent a business context, a critical or important function, a process area or a security domain.

The detailed information is not stored on the Security Space itself. Business properties, ICT service attributes, classifications, risks and other object-specific information remain on the relevant information objects. Control status, evidence and follow-up are managed in the associated control plans. The Security Space provides the protected context, access boundary and aggregation layer for reporting across the objects it groups.

For financial entities subject to DORA, Security Spaces can be used to structure and protect operational areas that are central to digital operational resilience. Examples include:



Financial sector context	Stored on
Payments	Payment process, payment platform, clearing service, authentication service, customer account data, payment operations team
Credit management	Credit application process, credit scoring service, customer data, decision engine, case management system, credit department
Customer onboarding / KYC	KYC process, AML screening service, identity verification provider, customer documentation, compliance team
Trading and market operations	Trading platform, order management system, market data service, settlement process, trading operations team
Insurance claims	Claims handling process, claims system, customer and policy data, external claims service provider, claims department
Core banking	Core banking platform, account ledger, customer account process, integration services, IT operations team
Digital channels	Mobile banking app, internet banking platform, API gateway, authentication service, customer support process
ICT operations	Infrastructure services, cloud platform, monitoring service, privileged access management, IT operations team
Third-party ICT services	Outsourced operations, SaaS services, cloud providers, managed security services, supplier management process

A Security Space provides the structural and access-control context for the objects that are relevant to a specific business or operational area. For example, a Security Space for “Payments” may group the payment process, the payment platform, the authentication service, the customer account information set and the payment operations unit. A Security Space for “Customer onboarding” may group the KYC process, identity verification services, AML screening tools, customer documentation and the compliance function.

For DORA purposes, this makes it possible to group the objects that together support a critical or important function. The Security Space defines the protected context and determines which groups and roles can access and work with the relevant objects. This is particularly useful in financial organisations where responsibility is often shared between business owners, system owners, ICT operations, compliance, risk management, data protection and internal audit.

Security Space also supports aggregated reporting. Since risks in DirSys are connected to the information objects they affect, the Security Space can be used to report the combined risk picture for all objects within a selected business context, critical function or operational area. This allows an organisation to analyse DORA-related exposure not only per individual object, but also across the full set of processes, ICT services, information assets and organisational responsibilities that support a financial service.

In practical terms, Security Space enables DirSys to combine object-level governance with aggregated oversight. Risks remain attached to the information objects where they arise, while Security Space and Insights make it possible to visualise and report the overall risk and control status for the wider operational context.

2.1 DORA implemented through the rule engine

The rule engine is the key to making DORA practical. Instead of asking users to manually select every applicable DORA control, DirSys can evaluate object properties and automatically activate relevant control plans, controls, risks and suggested actions.

2.2 Example: Payment system under DORA

Object: Payment system

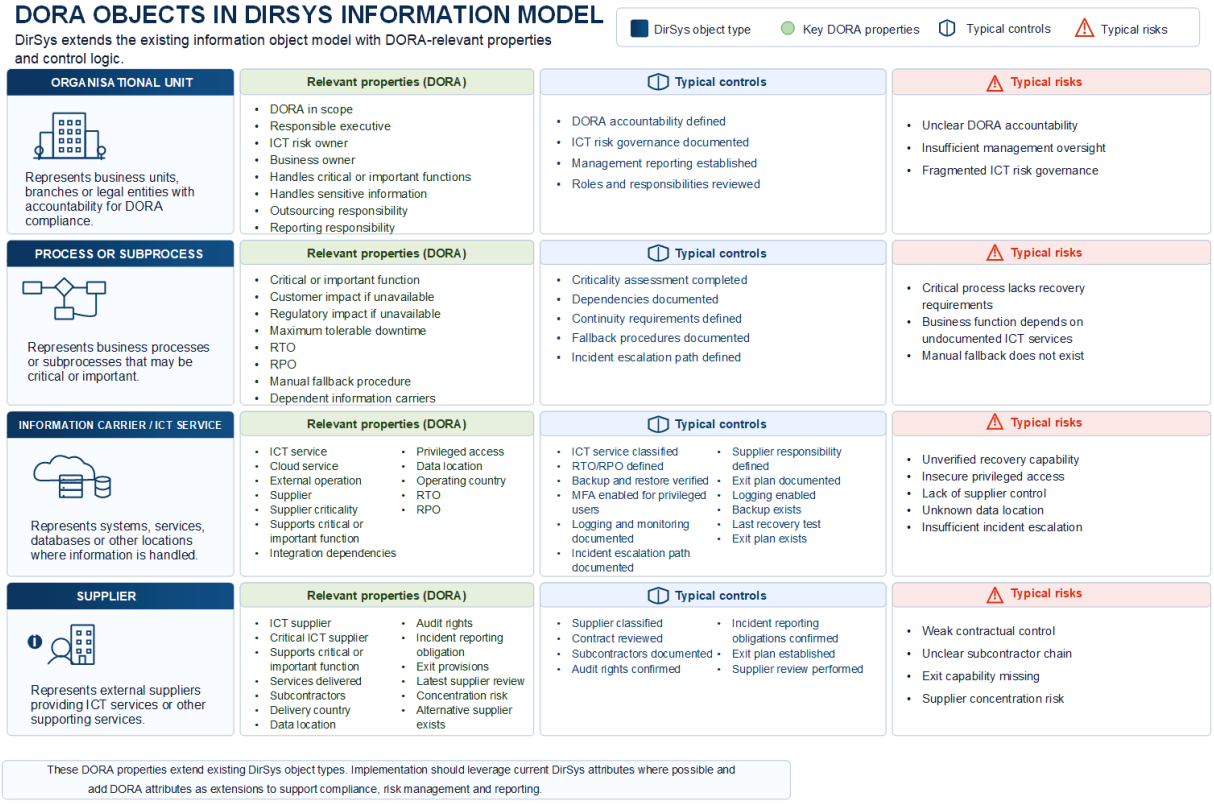
Properties:
- Supports critical or important function = Yes
- External ICT provider = Yes
- Cloud service = Yes
- Recovery test older than 12 months = Yes

Rule engine result:
- Control plan: DORA - ICT service resilience
- Control: Define and verify RTO/RPO
- Control: Perform recovery test
- Control: Review supplier obligations
- Risk: Unverified recovery capability
- Risk: Critical supplier dependency
- Action: Schedule recovery test and update evidence

This is more powerful than a traditional GRC checklist because the controls are activated by the real structure and risk profile of the organisation.

3 Recommended DORA object properties

DirSys does not need a completely separate DORA data model. It should extend the existing information object model with DORA-relevant properties.



3.1 Organisational unit

Relevant properties	Typical controls	Typical risks
- **DORA in scope** - **Responsible executive** - **ICT risk owner** - **Business owner** - **Handles critical or important functions** - **Handles sensitive information** - **Outsourcing responsibility** - **Reporting responsibility**	- DORA accountability defined - ICT risk governance documented - Management reporting established - Roles and responsibilities reviewed	- Unclear DORA accountability Insufficient management oversight - Fragmented ICT risk governance

3.2 Process or subprocess

Relevant properties	Typical controls	Typical risks
- **Critical or important function** - **Customer impact if unavailable** - **Regulatory impact if unavailable** - **Maximum tolerable downtime** - **RTO** - **RPO** - **Manual fallback procedure** - **Dependent information carriers** - **Dependent ICT suppliers**	- Criticality assessment completed - Dependencies documented - Continuity requirements defined - Fallback procedures documented - Incident escalation path defined	- Critical process lacks recovery requirements - Business function depends on undocumented ICT services - Manual fallback does not exist

3.3 Information carrier / ICT service

The existing DirSys model already treats information carriers as systems, services, databases or other locations where information is handled. For DORA, this should be extended or formalised with the following properties and control logic.

Relevant properties	Typical controls	Typical risks
- **ICT service** - **Cloud service** - **External operation Supplier** - **Supplier criticality** - **Supports critical or important function** - **Integration dependencies** - **Privileged access** - **Data location** - **Operating country** - **RTO** - **RPO**	- ICT service classified - RTO/RPO defined - Backup and restore verified - MFA enabled for privileged users - Logging and monitoring documented - Incident escalation path documented - Supplier responsibility defined -Exit plan documented - Logging enabled - Backup exists - Last recovery test - Exit plan exists	Unverified recovery capability Insecure privileged access Lack of supplier control Unknown data location Insufficient incident escalation

3.4 Supplier

Supplier can either be treated as a structured property on an information carrier or, preferably for DORA, as a separate object type.

Recommended supplier properties	Typical controls	Typical risks
- **ICT supplier** - **Critical ICT supplier** - **Supports critical or important function** - **Services delivered** - **Subcontractors** - **Delivery country** - **Data location** - **Audit rights** - **Incident reporting obligation** - **Exit provisions** - **Latest supplier review** - **Concentration risk** - **Alternative supplier exists**	- Supplier classified - Contract reviewed - Subcontractors documented - Audit rights confirmed - Incident reporting obligations confirmed - Exit plan established - Supplier review performed	- Weak contractual control - Unclear subcontractor chain - Exit capability missing - Supplier concentration risk

4 DORA control plans

DORA should be implemented in DirSys as a framework with object-specific control plans.

Control plan	Applies when
DORA - Governance	Organisational unit is DORA in scope
DORA - Critical or important function	Process is marked as critical or important
DORA - ICT service resilience	Information carrier is DORA relevant
DORA - Cloud service	Information carrier is a cloud service
DORA - Third-party ICT risk	External ICT provider is involved
DORA - Incident readiness	Object supports critical or important function
DORA - Continuity and recovery	Process or ICT service is critical
DORA - Information register quality	Object is DORA relevant
DORA - Management reporting	Organisational unit or function is in scope

DirSys

5 Example DORA rules

Rule 1: Cloud service supporting critical function

IF
Information carrier.Cloud service = Yes
AND Information carrier.Supports critical or important function = Yes

THEN
Activate control plan: DORA - Cloud service
Activate control: Privileged access must use MFA
Activate control: Logging and monitoring must be documented
Activate risk: Insecure access to critical ICT service
Suggest action: Enable MFA and attach evidence

Rule 2: Critical process without fallback

IF
Process.Critical or important function = Yes
AND Process.Manual fallback procedure = No

THEN
Activate control: Manual fallback procedure must be documented
Activate risk: Critical function lacks operational fallback
Suggest action: Define and test fallback procedure

Rule 3: External supplier for critical ICT service

IF
Information carrier.External operation = Yes
AND Information carrier.Supports critical or important function = Yes

THEN
Activate control plan: DORA - Third-party ICT risk
Activate control: Supplier review must be completed
Activate control: Incident reporting obligations must be documented
Activate control: Exit plan must exist
Activate risk: Critical dependency on external ICT supplier

Rule 4: Recovery test missing

IF
Information carrier.DORA relevant = Yes
AND Information carrier.Last recovery test is older than 12 months

THEN
Activate control: Recovery test must be performed
Activate risk: Recovery capability is not verified
Suggest action: Schedule and document recovery test

Rule 5: Register quality issue

IF
Information carrier.DORA relevant = Yes
AND Supplier is empty

THEN
Activate control: ICT supplier must be documented
Activate risk: Incomplete DORA information register
Suggest action: Complete supplier information

6 DORA information register

DirSys should not require users to maintain a separate DORA register manually. Instead, the register should be generated from information objects, object properties, Security Space grouping, control plan status, risks, actions and evidence.

DORA register need	DirSys source
Critical or important function	Process / subprocess
ICT service	Information carrier
Supplier	Supplier object or supplier property
Contract status	Supplier or contract control plan
Data location	ICT service property
RTO/RPO	Process or information carrier property
Recovery test status	Control plan
Third-party risk	Supplier risk
Incident readiness	Incident control plan
Evidence	Control point evidence
Open remediation	Actions

This approach makes the register a by-product of operational governance, not a separate administrative burden.

7 Insights and reporting

Insights should provide DORA-specific dashboards and management views. This allows operational owners, compliance teams, management and auditors to work from the same underlying data.

Dashboard	Example metrics
DORA executive dashboard	- Number of critical or important functions - Number of DORA-relevant ICT services - ICT services without defined RTO/RPO - Critical services without recent recovery test - External ICT suppliers supporting critical functions - Suppliers without completed review - Open high ICT risks - Overdue DORA actions - Control plan completion by business area
DORA register quality dashboard	- DORA-relevant systems without supplier - Critical processes without system mapping - ICT services without data location - Suppliers without subcontractor information - Critical services without exit plan Objects without assigned owner Controls without evidence
DORA risk dashboard	- Risk exposure by process - Risk exposure by supplier - Risk exposure by ICT service - Risks created by missing controls - Trend of residual ICT risk over time

8 Role and access model

Because Security Space is connected to groups and permissions, DirSys can use the same structure for access control and accountability.

Group	Access through Security Space	Typical role
CISO group	All DORA-relevant objects	Overall ICT risk governance
HR group	HR-related objects	Business ownership
IT operations	ICT services and infrastructure	Technical remediation
Data protection coordinator	Objects with personal data	Data protection perspective
Supplier management	Supplier-related objects	Third-party risk follow-up
Internal audit	Read-only access	Independent review

9 Why the DirSys model is well suited for DORA

Traditional compliance tools often start with a regulatory checklist. That can create a gap between the regulation and the actual business environment. DirSys starts from the organisation's own structure:

- Organisational units
- Processes
- Subprocesses
- Systems
- Services
- Information assets
- Suppliers
- Control plans
- Risks
- Actions
- Evidence

The rule engine then applies relevant controls based on object properties. This creates several advantages:

- Controls become context-aware.
- Risk is linked to real business objects.
- Responsibilities can follow existing groups and roles.
- Evidence is stored where the control is managed.
- Reporting can be generated from live operational data.
- The DORA register can be produced from the same data model.

10 Verifying and demonstrating operational resilience

A central part of DORA is the ability to demonstrate that governance, controls and risk management work in practice — not only that they are documented. Organisations must be able to verify the actual status across systems, identities, suppliers and operational environments.

This is where the broader DirSys model becomes valuable. DirSys Core provides the governance foundation by managing information objects, Security Spaces, frameworks, control plans, risks, actions, evidence and reporting. It defines what needs to be governed, which controls apply, who is responsible and how follow-up should be managed.

SecurityHub extends this model with technical verification. By connecting to identity and access sources, directory services, identity providers, cloud platforms and application interfaces, SecurityHub can verify whether selected controls are fulfilled in the connected systems. This helps organisations move from self-assessment to evidence-based verification, where findings and deviations can be linked back to risks, control plans and actions in DirSys Core.

TrustCenter adds the transparency and supplier control layer. It allows organisations to publish selected governance information, policies, control status, evidence, register information and supplier assessments in a structured and controlled way. This supports both stakeholder transparency and ICT third-party risk management under DORA.

Together, DirSys Core, SecurityHub and TrustCenter create a connected operating model for DORA. DirSys Core acts as the governance engine, SecurityHub verifies selected controls against real operational data, and TrustCenter enables controlled transparency and supplier follow-up.

This is what makes the DirSys model distinctive:

DORA can be managed as an integrated governance process rather than as a separate spreadsheet, static checklist or isolated compliance project.