XOPERO
Backup&Recovery

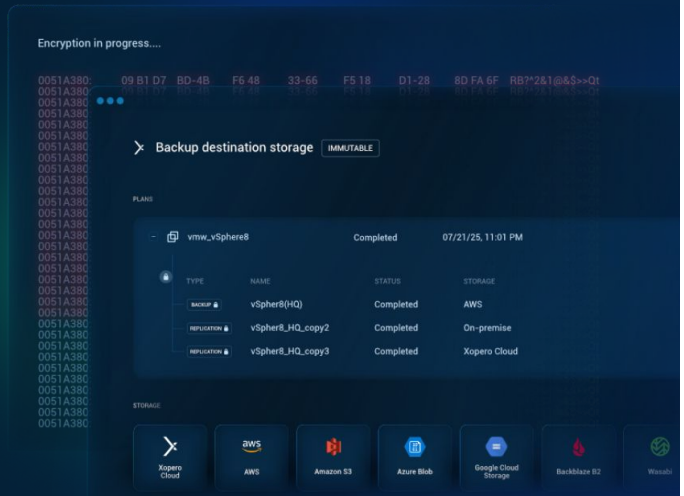
CAF 4.0 with Xopero

Strengthen backup, resilience and recovery for **essential services**



XOPERO
Backup&Recovery

CAF 4.0: Cyber resilience for essential services



The NCSC Cyber Assessment Framework helps organisations assess how well they manage cyber risk to essential functions.

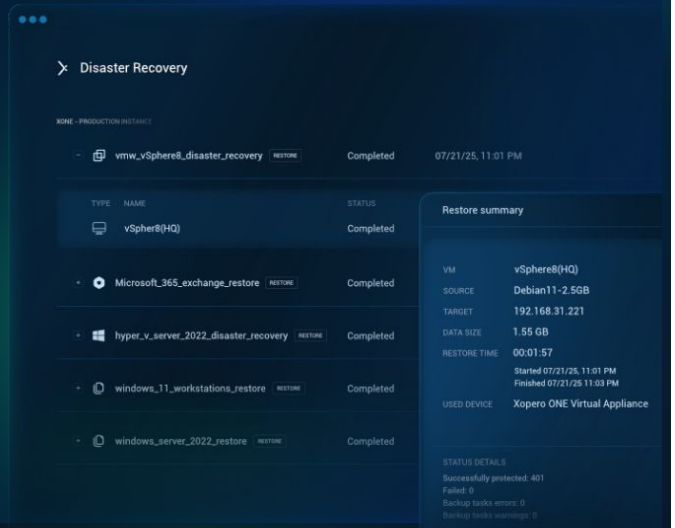
CAF is primarily designed for organisations operating essential services, including energy, healthcare, transport, digital infrastructure and government. It is used by nearly all UK cyber regulators and in government through GovAssure.

CAF 4.0 comprises 4 objectives, 14 principles and 41 contributing outcomes. It focuses on outcomes and leaves organisations to choose the controls that fit their environment.

Several CAF outcomes address backup, data protection, resilience and recovery. These are also the areas where Xopero provides its strongest technical support.

XOPERO
Backup&Recovery

Xopero: backup and recovery for IT, DevOps and ICS/OT



Xopero Software has developed backup and recovery technology in Europe since 2009. The company is ISO/IEC 27001 certified and has completed an independent SOC 2 Type II audit.

Xopero ONE
Central backup and recovery management software for physical, virtual, cloud and hybrid infrastructure.

Xopero Unified Protection
A preconfigured appliance combining Xopero ONE with dedicated backup storage, archiving and deduplication.

Xopero Sphere Recovery Drive
Offline backup and local recovery for isolated ICS/OT systems, including recovery without network access.

GitProtect
Automated backup and disaster recovery for DevOps.

How Xopero supports core CAF backup and recovery requirements

CAF objective/principle	Put it into practice with Xopero	Use these Xopero capabilities
Objective B/ B5.c Backups Keep current, secured and accessible backups of the data needed to recover essential functions. Backups should be automated, tested and reviewed. regularly	**Run backup as a controlled, repeatable process across your infrastructure.** Apply protection rules centrally and consistently. Quickly identify systems that fall below the required protection levels.	• policy-based backup • advanced backup schemes • retention & versioning • central monitoring • SLA reports
Objective B/ B3.c Stored Data Protect important stored data against unauthorised access modification and deletion. Backups must remain secure and usable for recovery.	**Keep recovery data protected if production is compromised.** Separate the recovery layer form risks affecting primary systems.	• AES encryption with private key • immutable/WORM storage • non-executable backup format • restricted storage credentials
Objective D/D1.b - Response and Recovery Capability Maintain recovery capability when primary systems fail or become unavailable.	**Match the recovery path to the incident and the system affected.** Keep recovery options available for connected IT and isolated ICS/OT environments.	• granular & point-in-time restore • Instant Disaster Recovery • Any2Any Restore • remote Bare Metal Restore • Sphere Recovery Drive

How Xopero supports CAF resilience and recovery readiness

CAF objective/principle:	Put it into practice with Xopero	Use these Xopero capabilities
Objective B/ B5.b Design for Resilience Reduce dependencies, resource constraints and geographical weaknesses that could disrupt essential functions.	**Separate recovery from production and reduce single points of failure.** Keep recovery data and the backup platform available through disruption.	• multi-storage • replication & geo-redundancy • Air Gap • immutable/WORM storage • automatic failover
Objective B/ B5.a Resilience Preparation Prepare BC/DR arrangements based on what must be recovered, in what order and within what time.	**Standardise recovery before an incident.** Reduce integration work and simplify recovery operations.	• ready-to-use BCDR appliance • integrated backup storage • central management console • automatic updates • one-vendor support
Objective D/D1.c Testing and Exercising Test response and recovery arrangements to confirm that they work in practice.	**Check the technical recovery path before you need it.** Keep evidence that can be reviewed later.	• scheduled test restore • VM startup check • post-start screenshot • RTO/RPO measurement • test restore history

How Xopero supports CAF security and assurance requirements

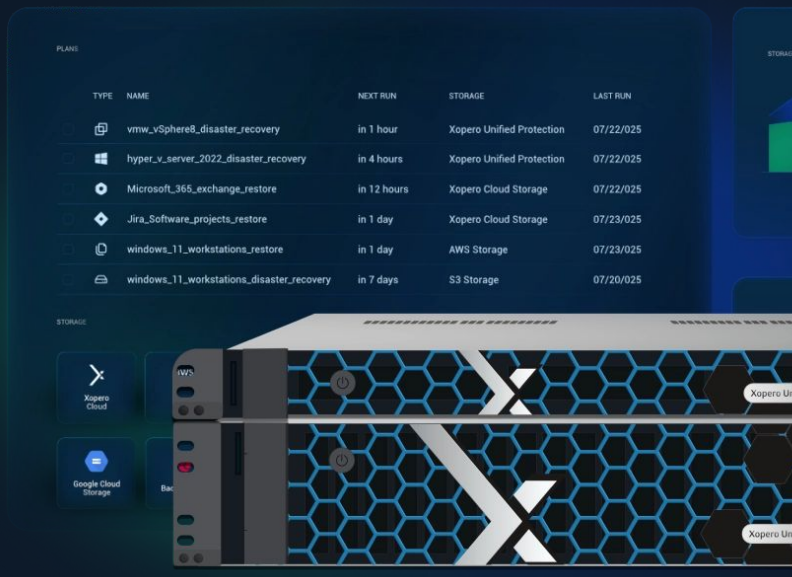
CAF objective/principle	Put it into practice with Xopero	Use these Xopero capabilities
Objective B/ B2.d Identity and Access Management (IdAM) Give users only the access they need and keep access rights under control.	**Apply least-privilege access to backup and recovery.** Tie access to corporate identity and job responsibilities.	• role-based access • separate admin/backup/restore roles • granular permissions • SAML group mapping
Objective B/ B3.b Data in Transit Protect important data while it moves across networks, particularly over untrusted connections.	**Keep backup traffic protected across local and cloud transfer paths.**	• source-side encryption • encrypted transfer
Objective A/ A2.c Assurance Validate that security controls remain effective and provide evidence for review.	**Keep protection status visible and act quickly when something needs attention.** Retain evidence for later review.	• compliance dashboard • SLA reports • advanced logs • e-mail/Slack/webhook alerts • task history

XOPERO
Backup&Recovery

Want to move more CAF outcomes towards ‘Achieved’?

- See Xopero in action.
- Discuss your recovery priorities,
- and explore the right setup for your environment.

Book a demo



This material is for general information only. It does not constitute legal, regulatory, or compliance advice. Any CAF assessment must consider the organisation's specific processes, architecture, risk profile, and regulatory obligations.