LSSCO SECURE OPERATIONS

Secure operational control across connected buildings and active projects.

A practical management method for ownership, connected assets, vendor access, evidence, incident responsibility, recovery and handover.

LSSCO leads the operational review. Uriyel SiteWorks supports the evidence and action record. Qualified technical providers perform specialist testing, monitoring and engineering where separately authorized.

info@lsscoltd.com | +44 7432 364440 | www.lsscoltd.com

01 / PURPOSE

The operating gap.

A project can look controlled while its connected and digital dependencies remain unmanaged.

01 / ACCESS

Access without ownership.

Shared or former vendor accounts remain active without a business sponsor, review date or removal decision.

02 / EVIDENCE

Records without provenance.

Approvals, exports and configuration evidence can be altered, deleted or separated from the source record.

03 / CONNECTED ASSETS

Technology without lifecycle control.

CCTV, access control, Wi-Fi and building platforms are installed without an owned support and recovery model.

04 / RESPONSE

Incidents without a route.

No one knows who contains vendor access, preserves records, informs the owner or verifies restoration.

METHOD OBJECTIVE

One accountable operating picture.

Bring people, systems, vendors, evidence and connected assets into the same responsibility structure before handover gaps become business risk.

info@lsscoltd.com | +44 7432 364440 | www.lsscoltd.com

02 / MANAGEMENT STRUCTURE

Six continuous functions.

Govern, Identify, Protect, Detect, Respond and Recover organize cybersecurity outcomes as a continuous management structure. Their order does not impose a project sequence; activities may run concurrently according to risk and operating need.

01 / GOVERN

Set ownership and boundaries.

Risk owners, decisions, vendor obligations, escalation and accepted operating position.

02 / IDENTIFY

Understand the environment.

Users, information, connected assets, providers, dependencies and critical services.

03 / PROTECT

Apply proportionate safeguards.

Identity, privilege, separation, configuration, backups and vendor connectivity.

04 / DETECT

Define useful visibility.

Evidence sources, events, recipients and review cadence supplied by technical parties.

05 / RESPOND

Coordinate decisions.

Incident leadership, containment authority, records, communication and remediation.

06 / RECOVER

Restore and verify.

Service priorities, recovery evidence, restoration validation and owner acceptance.

info@lsscoltd.com | +44 7432 364440 | www.lsscoltd.com

03 / CONTROL DOMAINS

Eight domains form the managed record.

The review connects technical requirements to business ownership, evidence sources and corrective action.

01

Identity and access

Named users, roles, privileges, sponsors, review dates and removal.

02

Environment separation

Client, property, project and vendor boundaries across interfaces.

03

Evidence provenance

Source, custodian, timestamp, version and provider-supplied integrity evidence.

04

Vendor control

Purpose, named contact, access route, duration, review and offboarding.

05

Connected assets

Owner, dependency, support, lifecycle and recovery requirement.

06

Monitoring requirement

Events that matter, observing provider and management evidence route.

07

Incident readiness

Lead, deputy, authority, contacts, communication and evidence route.

08

Recovery and handover

Configuration records, restoration tests, transfer pack and acceptance.

info@lsscoltd.com | +44 7432 364440 | www.lsscoltd.com

04 / DELIVERY

Mobilize through owner transfer.

The method follows the environment from first scope through controlled handover without pretending that LSSCO directly operates every underlying system.

01

Mobilize

Define scope, owner, services, users, vendors and professional boundaries.

02

Map

Create the system context, asset register, access matrix and dependency record.

03

Control

Prioritize identity, evidence, vendor, configuration and recovery requirements.

04

Exercise

Use a safe scenario to test authority, communication, containment and restoration.

05

Report

Issue executive findings, responsible parties, referrals and owner decisions.

06

Transfer

Handover ownership, open risks, recovery evidence and the 90-day action route.

TECHNICAL BOUNDARY

No unapproved penetration test, vulnerability scan, continuous monitoring, digital forensics, network engineering, building-controls engineering, safety-critical system test or formal compliance certification is included in the standard review.

info@lsscoltd.com | +44 7432 364440 | www.lsscoltd.com

05 / FIRST ENGAGEMENT

Begin with one defined environment.

The Connected Facility Review is a management and readiness engagement, not an unapproved technical test.

01

Defined scope

One building, project, platform or operational workflow.

02

Operating map

People, systems, vendors, data, assets and critical dependencies.

03

Control position

Ownership, access, evidence, incident and recovery gaps.

04

Decision pack

Priority actions, responsibilities, technical referrals and 90-day route.

PROFESSIONAL BOUNDARIES

- Technical testing requires separate written scope, authority and appropriate competence.
- Fire, lift, alarm, access, BMS and related safety-critical systems remain with appointed competent parties.
- LSSCO does not replace legal, engineering, code, fire-safety, privacy, IT-management, certification or regulatory roles.
- References to NIST or CISA do not mean certification, accreditation, endorsement or compliance by association.

info@lsscoltd.com | +44 7432 364440 | www.lsscoltd.com