FirstWave

Automating Compliance with Foundations for OT Cybersecurity: Asset Inventory Guidance

How Open-AudIT helps critical infrastructure operators simplify compliance with automated asset discovery and management

Introduction: Why Asset Inventory Matters for OT Cybersecurity

Operational Technology (OT) systems are the backbone of critical infrastructure. From energy and water to transport and manufacturing, these environments depend on reliable and secure OT assets. As more devices become connected, the risk of cyber disruption grows.

To help operators strengthen defences, the **Australian Cyber Security Centre (ACSC)** has released the **Foundations for OT Cybersecurity: Asset Inventory Guidance.** This framework outlines how owners and operators should create and maintain an OT asset inventory. Its purpose is simple but essential: **you cannot defend what you cannot see.**

The guidance sets clear expectations:

- Define the scope and objectives of an asset inventory.
- Identify authorised, unauthorised, and unmanaged assets.
- Collect detailed attributes such as hardware, software, and configurations.
- Classify assets by role, location, or criticality.
- Manage the data lifecycle with governance and regular updates.
- Use the inventory to support risk, compliance, and operational performance.

For many organisations, meeting these requirements will be a significant challenge. Manual methods—like spreadsheets or site audits—are slow, resource-heavy, and outdated almost as soon as they're complete. In complex OT and hybrid IT/OT environments, this creates blind spots that attackers can exploit, and regulators cannot overlook.

This is where automation becomes critical. Tools like **Open-AudIT,** FirstWave's network discovery and inventory solution, help operators build a **trusted, continuously updated asset inventory.** By automating discovery, classification, and reporting, Open-AudIT turns compliance into a repeatable process rather than a one-off burden.

In this article, we'll cover:

- The **main challenges organisations face** when complying with the ACSC guidance.
- How **Open-AudIT automates asset inventory** to address those challenges.
- The **real-world benefits** for operators of critical infrastructure adopting an automated approach.

By combining compliance requirements with automation, organisations can transform asset inventory into a **strategic enabler of cyber resilience.**

The Challenges Organisations Face in Compliance

The ACSC's **Foundations for OT Cybersecurity: Asset Inventory Guidance** provides a strong framework, but implementation is not straightforward. Many organisations struggle to meet the requirements due to gaps in visibility, governance, and process.

1. Visibility Gaps and Legacy Systems

Most OT environments run on a mix of modern and legacy systems. Many of these devices use proprietary protocols or are air-gapped, making them hard to detect with traditional IT tools.

- Legacy PLCs and ICS often lack native cybersecurity features.
- Air-gapped or non-IP devices may not show up in discovery scans.
- Blind spots increase the risk of unmanaged or unauthorised assets.

2. Defining Scope, Governance, and Ownership

An inventory is only as strong as its governance. Many organisations struggle to agree on scope and responsibility.

- IT and OT teams often work in silos.
- No clear ownership leads to inconsistent updates.
- Governance gaps result in fragmented inventories.

3. Collecting Detailed Asset Attributes

The guidance requires detailed information such as hardware specs, installed software, network data, and ownership. Collecting this manually is resource-intensive and often out of date before completion.

4. Building Effective Taxonomy and Classification

Assets must be grouped by role, location, or criticality. Each organisation has unique structures, making a one-size-fits-all taxonomy ineffective. Without automation, classification is static and hard to maintain.

5. Centralising Data and Managing Lifecycle

Asset data is often siloed in spreadsheets or vendor documents. This prevents lifecycle tracking and leads to duplication, inconsistencies, and missed decommissioning updates.

6. Training and Awareness Challenges

OT teams may lack cybersecurity knowledge, while IT teams may not understand OT systems. Without training and awareness, asset inventory processes lose momentum.

7. Integrating Asset Inventory into Risk and Operations

Static inventories don't add value to risk management or operations. Without integration into monitoring and reporting, inventories become shelfware rather than a living resource.

How Open-AudIT Supports Compliance

Meeting the ACSC guidance requires automation. **Open-AudIT** is built to address the challenges of asset visibility, governance, and lifecycle management.

1. Automated Discovery Across IT, OT, and Cloud

- Agent and Agentless discovery.
- Identifies all devices - managed, unmanaged, and rogue.
- Integrations for AWS, Azure, and Google Cloud.

2. Governance, Scope Definition, and RBAC

- Define organisations, sites, and locations.
- Custom fields for tracking ownership and compliance categories.
- Role-based access control (RBAC) with LDAP/SSO.

3. Detailed Attribute Capture and Change Detection

- Hardware, software, IP, MAC, ports, antivirus, and firewall details.
- Change detection tracks modifications in configurations.

4. Flexible Taxonomy with Tagging and Classification

- Tag assets by role, function, criticality or any other critical attribute.
- Group assets by operational priority, business unit or any other attribute.
- Visualise grouped assets in dashboards and reports.

5. Central Repository, Automation, and Baselining

- Single source of truth for all discovered assets.
- Scheduled scans and automated updates.
- Baseline comparisons highlight deviations.

6. User-Friendly Interface and Training Resources

- Web-based interface with dashboards and maps.
- Exportable reports in Excel/CSV, JSON, XML, and HTML.
- Extensive community documentation and support.

7. Reporting, API Integration, and NMIS Connection

- Custom compliance reports for audits.
- RESTful API for CMDB, SIEM, and governance integration.
- Integration with NMIS for real-time monitoring and event correlation.

Mapping Open-AudIT to the ACSC Functional Requirements

ACSC Requirement	How Open-AudIT Delivers
Define Scope & Objectives	Organisations, sites, custom fields, RBAC
Identify Assets	Agentless discovery across IT, OT, and cloud
Collect Attributes	Hardware/software, IP, MAC, ports, antivirus, change logs
Create Taxonomy	Custom tags, grouping, dashboards
Manage Data	Central repository, automation, export options
Lifecycle Management	Historical records, baselines, lifecycle accuracy
Cybersecurity & Risk Support	Compliance reports, alerts, NMIS/SIEM integration
Maintenance & Reliability	Alerts on new devices, config changes
Performance Monitoring & Reports	Dashboards, custom reporting, KPI alignment
Training & Awareness	User-friendly UI, documentation, community support
Continuous Improvement	Continuous scanning, updates, taxonomy refinement

Open-AudIT directly operationalises the ACSC framework, ensuring compliance is both achievable and sustainable.

Real-World Benefits for Critical Infrastructure Operators

Faster Compliance Cycles

Automated discovery and scheduled scans reduce compliance reporting from months to days.

Reduced Risk Exposure

Shadow assets, outdated software, and insecure configurations are quickly identified, reducing cyber risk.

Stronger Collaboration Between IT and OT Teams

Shared dashboards and role-based access enable IT and OT to work from a single source of truth.

Operational Efficiency Through Automation

Change detection, baselining, and integration with NMIS reduce manual effort and free staff for higher-value work.

Continuous Improvement

Continuous scanning and taxonomy refinement keep inventories current, supporting long-term resilience.

Conclusion: Automating Asset Inventory for Cyber Resilience

The ACSC guidance makes one point clear: **a complete, accurate, and continuously updated asset inventory is essential for cybersecurity and compliance.** Manual methods can't keep up, but automation with **Open-AudIT** makes it achievable.

Open-AudIT enables:

- **Automated discovery** across IT, OT, and cloud.
- **Rich attribute collection** with change tracking.
- **Custom taxonomy** aligned to real operations.
- **Centralised data** that integrates with risk and operations.

For operators of critical infrastructure, this means faster compliance, reduced risk, better IT/OT collaboration, and sustainable resilience.

Next Steps

If you're ready to turn asset inventory into a strategic enabler of compliance and resilience:

1. **Download Open-AudIT** and get started today.
2. Explore **Open-AudIT on FirstWave** to learn more about its capabilities.
3. Book a **demo or consultation** with our team to see how automation can simplify your compliance journey.

Automating compliance is no longer optional—it's the smarter, safer way forward.