

Switch configuration reviews are easy to defer. The network seems to be working, users can reach their applications, and nobody wants to risk an outage by touching a switch that has been stable for years. Then a new device appears on an unexpected VLAN, a trunk carries more traffic than intended, or an old account still has administrative access. The configuration may have changed gradually, but the security consequences can arrive all at once.

So, how often should you audit switch configs for security? For most organisations, the practical answer is: review them at least quarterly, check important changes as they happen, and reassess immediately after a significant incident or network change. Higher-risk environments may need more frequent automated checks. The right schedule depends on the role of the switches, the sensitivity of the systems they connect, and how well changes are controlled.

A switch configuration review is not just a line-by-line check of commands. It should test whether the intended network design still exists, whether access is appropriately restricted, and whether the physical infrastructure supports the security controls you believe you have. In my experience, a tidy configuration on paper can be undermined by an unlabelled patch panel, an unmanaged switch under a desk, or a link that nobody remembers installing. Mystery cables are a security smell.

Why switch configuration reviews matter

Switches enforce important boundaries inside a network. They determine which ports are active, which devices can connect, how VLANs are assigned, and which traffic can cross between segments. If these controls are weak or have drifted from the design, an attacker who gains access to one device may have a much easier path to other systems.

That risk is not limited to office computers. Corporate networks often share sites, comms rooms or support processes with building management, manufacturing, laboratory or other operational technology (OT) systems. A compromised endpoint may be a foothold into infrastructure that was meant to be isolated. In those environments, a mistaken VLAN assignment or an unintended trunk can have safety, availability and business consequences as well as security ones.

Segmentation depends on capable switching and correct design. A VLAN alone is not a complete security boundary: routing, access control lists, firewalls and management access all need to be considered. Nor does buying a capable switch automatically create good segmentation. The configuration has to match the design, and the design has to be maintained as equipment, users and workloads change.

That is why ACSC guidance should be considered alongside the real state of your network. Guidance on secure configuration, access control, asset management and network protection assumes that you have a reasonably understood, controlled foundation. If you do not know what is connected to a switch, or which ports carry traffic between security zones, written policy cannot compensate for that uncertainty.

How often should you audit?

A useful starting point is a risk-based cadence rather than one fixed interval for every switch. Put the review schedule in your security or network operations calendar, name an owner, and make sure the review produces evidence: the configuration examined, findings raised, and actions completed or accepted as risks.

Review activity	Suggested frequency	What it should cover	Automated configuration and change checks
Daily or weekly, where tooling permits	Unexpected changes, configuration backups, approved-baseline comparisons and critical alerts	Formal switch configuration review	At least quarterly
Management access, VLANs, trunks, unused ports, logging, protocols and security settings	High-risk or critical infrastructure review	Monthly or after material changes	Switches supporting OT, sensitive services, internet-facing infrastructure or key security boundaries
Full design and physical review	Annually, and after major site changes	Whether cabling, diagrams, port assignments and segmentation still reflect the approved design	

These intervals are a sensible baseline, not a substitute for risk assessment. A small office with a well-managed network may not need a monthly manual audit of every access switch. A plant network supporting continuous operations may warrant tighter checks, especially where change windows are limited or vendor access is involved.

Whatever cadence you choose, review changes when they are made, not only when the next audit comes around. A quarterly audit cannot reliably catch a dangerous change that was introduced yesterday and remains in place for three months. Use change control, configuration backups and alerts to shorten that gap.

What should a switch configuration review check?

Start with the intended design and compare it with the live configuration. Do not simply search for a list of “secure” commands. A setting can be technically secure yet break a business service, while a configuration that looks familiar may be inappropriate for a particular switch or network zone.

1. Administrative access and default credentials

Check that default credentials have been removed and that administrative access is limited to authorised people and management systems. Default credentials are a basic but persistent risk, particularly on devices installed in a hurry or equipment that has been reset for troubleshooting. Use unique credentials, strong authentication where supported, and centralised identity controls where practical.

Also review which management protocols are enabled and where they can be reached from. Prefer encrypted management methods and restrict access to a dedicated management network or approved administrator addresses. Disable unused services. Confirm that accounts are still required, that vendor access has an owner and expiry, and that old accounts are not quietly accumulating.

2. VLANs, trunks and segmentation drift

Compare VLAN assignments with the approved port and network design. Look for unexpected access ports, trunks carrying unnecessary VLANs, overly broad native VLAN settings, and ports that have been repurposed without updating the documentation. These are common sources of segmentation drift: the difference between the boundaries you intended and the ones the network currently enforces.

Verify the path traffic takes between segments. Switches may provide separation at Layer 2, but communication between VLANs is usually controlled by a router, layer-three switch or firewall. Check that those controls still enforce the intended policy. If firewalls are expected to mediate traffic between user, server, guest and OT networks, confirm that a change to switching has not created an alternate route around them.

3. Ports, protocols and resilience

Identify unused ports and confirm they are disabled or placed in an appropriately restricted state. Review protections against unauthorised devices and accidental loops, as suitable for the environment. Check spanning-

tree settings, link aggregation, discovery protocols and other features against the design and vendor guidance. Do not blindly disable protocols that operations or monitoring depends on; understand their purpose first.

Look for configuration inconsistencies across switch stacks and sites. A single switch with different access controls or VLAN handling can become the weak link. Confirm that redundant paths behave as intended and that monitoring will detect a failed link or unexpected topology change.



4. Logs, time and configuration backups

Verify that switches send useful logs to a central system, use a reliable time source and retain enough information for investigations. Confirm that configuration backups are recent, protected from unauthorised alteration, and usable for recovery. A backup that has never been tested is a hopeful assumption, not a recovery plan.

Review alerts for configuration changes and make sure they can be linked to an approved change record. If a switch changes at 2am, someone should be able to answer whether it was an authorised maintenance task, an automated process or an incident.

The physical layer is part of cybersecurity

Physical infrastructure is not separate from cybersecurity. A switch configuration can be correct while the cabling around it creates a blind spot. An undocumented patch lead may connect two areas that were meant to remain separate. An unmanaged switch can add ports outside your normal controls. A faulting fibre link can cause intermittent connectivity that encourages staff to install an unofficial workaround.

Physical layer faults create both outages and security blind spots. When links flap or a switch is overloaded, monitoring may become incomplete, devices may move between ports, and incident responders may struggle to establish what was connected where. In a messy comms room, even a straightforward investigation can turn into a guessing game. "It was working before the cabling tidy-up" is not an incident record.

Include a physical check in site reviews: compare labels and patching with diagrams, trace unexpected links, identify unmanaged devices, and confirm that cabinets and network rooms have appropriate access controls. Keep port

descriptions and patch-panel labels current. I keep a cyberdaily.au label maker in my laptop bag because “we’ll label it later” has a remarkable ability to become permanent.

Equipment, tools and operational context

Review devices according to their function, support status and environment. Cisco equipment may be part of a corporate campus or data-centre design; industrial switches from MOXA may sit closer to control systems; Garland technologies may be used in network visibility or traffic-access architectures. Their roles are different, so their configurations and review criteria should be appropriate to the job they perform. Do not assume one checklist fits every platform.

Use the information you already have. Configuration management and network monitoring tools can compare running configurations against approved baselines, flag changes and help identify devices that have disappeared or appeared. Firewalls provide another important control and source of evidence, but they cannot fix an unintended Layer 2 path or an unmanaged switch plugged in behind them.

Endpoint detection platforms can help identify suspicious behaviour on managed endpoints, but they do not replace switch security. Many infrastructure devices do not run endpoint agents, and an endpoint alert may not explain how an attacker reached a sensitive segment. Correlating endpoint alerts with switch logs, firewall events and configuration changes gives responders a fuller picture.

A practical review process

1. **Build an accurate inventory.** Record switch models, locations, owners, software versions, support status and the networks they serve. Include OT and edge equipment, not just the devices visible in the main corporate monitoring console.
2. **Define the approved baseline.** Document required management controls, segmentation rules, logging, port practices and exceptions. Keep the baseline specific enough to test, but allow documented differences where business or technical needs justify them.
3. **Collect and compare configurations.** Use secure backups and, where possible, automated comparison. Investigate differences rather than treating every deviation as either harmless or malicious.



4. **Validate the physical and logical picture.** Compare diagrams, port descriptions and patching with what is actually installed. Follow up on unknown devices and unexplained links.
5. **Prioritise findings by risk.** An exposed management interface or an unintended route into an OT zone deserves faster attention than a minor documentation gap, although both may need action.
6. **Track remediation and exceptions.** Assign an owner and deadline. If a finding cannot be fixed immediately, record the reason, compensating controls and review date.

Make the cadence useful

The purpose of a switch configuration review is not to produce a spreadsheet that nobody reads. It is to keep the network aligned with its security design, spot changes that weaken controls, and make recovery and investigation more reliable. A quarterly formal review is a sensible starting point for many organisations, supported by automated checks and event-driven reviews after material changes.

Most importantly, treat switching, cabling and configuration as one security conversation. Segmentation depends on both sound design and capable equipment; physical faults can undermine visibility; and default credentials or unmanaged devices can bypass otherwise sensible controls. Document the network, review it regularly, and make sure someone can explain what happens at 2am when a link fails or an unexpected change appears.

If the answer depends on finding the one person who remembers which cable goes where, the review has already found something worth fixing.