esper

The IT Audit Checklist for Dedicated Devices

Managing a fleet of dedicated devices is complex, especially as you scale. Do you know how prepared your business is for IT failures? How about documentation and processes? If a dozen new devices show up today, are your processes for setting them up clear and repeatable? Regular IT audits can help you answer these questions and more.

This guide will cover 10 top-level points to focus on and why they're important. Regular IT assessments can keep your devices running smoothly, security tight, and processes aligned.

Table of Contents

01

Configuration Management

Configuration management involves looking closely at the processes around deploying and maintaining your devices. The process should be well-documented, easy to follow, consistent across devices, and follow industry best practices.

Why it's important

The health of your device fleet starts with proper configuration. Without repeatable processes, scaling your devices becomes slow and cumbersome while providing inconsistent experiences for the end user. The proper documentation will avoid these issues.

Questions to ask when auditing configuration management

- [ ] Is our configuration process well documented and easy to follow?
- [ ] Do our processes align with industry best practices?
- [ ] Is the user experience consistent across all devices?

02

Access Controls

An access control audit verifies that those who have access need access. This usually includes verifying account access, password reset policies, and multi-factor authentication requirements and is foundational when following a Zero Trust security policy.

Why it's important

It's way too easy to leave access enabled for people who don't need it — former employees, those who have moved to other departments, etc. Similarly, this is the time to check for weak or compromised passwords, as you're only as strong as your weakest password.

Questions to ask when auditing access controls

- [ ] Do all these employees need the access they have?
- [ ] Can we offer more granular access control options?
- [ ] Do we have a password reset or multi-factor authentication policy in place? Should we update or change it?

If you want to dig deeper into your MDM's security practices, our 42-point MDM Security Checklist is a great starting point. It raises the questions you need to ask about your MDM, key points to consider when evaluating your MDM's practices, and what to do when things aren't up to snuff.

Download the checklist

03

Update Practices

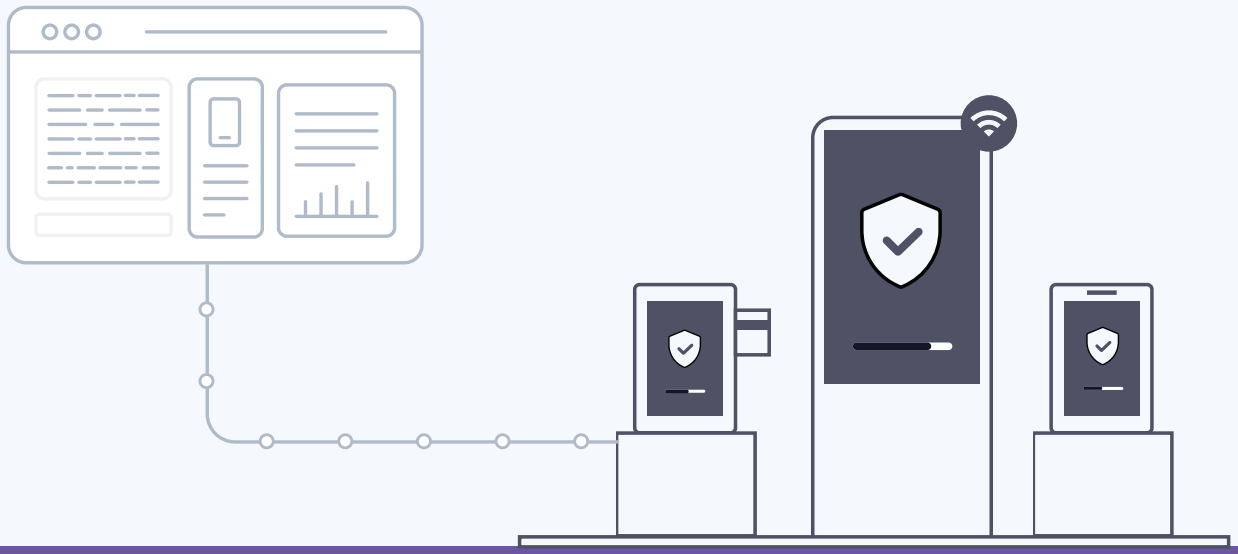
Update management (aka patch management) covers all the processes and procedures for applying updates to devices. It should cover everything from app updates to security patches and full system updates.

Why it's important

Updates are one of the most crucial aspects of managing a device fleet — they're your first and last line of defense regarding security, enable new features, and ensure devices and applications always run as well as they can.

Questions to ask when auditing update practices

- [ ] Do we have a repeatable, scalable system for delivering app updates? What about system updates and security patches?
- [ ] Do we release regular security patches to our apps and devices in compliance with best practices?
- [ ] Is this process documented?



04

Physical Security

Physical security audits encompass everything surrounding the actual devices themselves. From how they're deployed and secured on location to storage practices for unused assets — if it involves a physical device, you'll want to look at this.

Why it's important

Devices are company assets that cost money — not just the cost of the device itself, but the time it takes to set up and deploy. Ensuring your devices are physically secure is just as essential as digital security.

Questions to ask when auditing physical security

- [ ] Do we have physical security in place to prevent easy theft? Can our devices be tethered or locked to a single location?
- [ ] Do we have digital tracking to locate devices if they go missing?
- [ ] Are our extra or unused assets securely stored in a locked location? Who has access to this area?

05

Disaster Recovery

Auditing disaster recovery means looking at what happens if devices go down or get damaged. Many dedicated devices are business-critical, so this is the time to verify that you have a proven backup plan in case of an outage or emergency.

Why it's important

As more and more businesses rely on dedicated devices for day-to-day functions, they've moved away from many manual practices. Verifying that there's a backup plan in case something goes wrong ensures that business can continue and downtime is minimized.

Questions to ask when auditing disaster recovery

- [ ] Is there a documented backup plan for an internet or other device outage?
- [ ] Has this backup plan been battle tested? Is it effective, or does it need to be updated?
- [ ] Do we have a seamless plan to recover or replace devices quickly if one goes down?

06

Monitoring and Logging

Auditing monitoring and logging practices of your dedicated devices ensures proper monitoring techniques and regular logging processes as a result of that monitoring. This might include tracking uptime (and downtime), device status, connection status, and more.

Why it's important

As you scale your device fleet, manually monitoring every device isn't practical. Effective monitoring means tracking important device metrics automatically and regularly logging that data in a way that's repeatable and accessible. Advanced monitoring practices involve automated notifications if a device goes outside of pre-set parameters.

Questions to ask when auditing monitoring and logging practices

- [ ] Are we tracking essential device stats and logging those in a way that's accessible?
- [ ] Are there metrics or system statistics that we're not monitoring and should be to maximize device health?
- [ ] Do we have the capability to set up automated notifications when a device deviates from the baseline?

If you're looking for a better way to gather important information about what's going on with your devices — everything from battery status to Wi-Fi connection and software details — you need reliable device telemetry. Esper provides a detailed snapshot of every device in your hardware fleet in real-time, all in a single location.

Learn more about Esper's device telemetry

07

Data backup

Good data backup practices ensure you always have a copy of your dedicated devices' most recent datasets, applications, and other critical content. Auditing your data backup strategy ensures that these practices are robust and reliable.

Why it's important

The data collected and used on your dedicated devices is the backbone of your business. From how these devices work on your corporate infrastructure to the information they collect, having an always-on backup strategy ensures you never lose anything if a device goes down.

Questions to ask when auditing data backup practices

- [ ] Is our backup strategy current? Could it be improved?
- [ ] What data are we backing up? Is there anything that can be added?
- [ ] Are our backups air-gapped and redundant if something happens to the current backup sets?

08

Vulnerability Management

Vulnerability management doesn't end with providing app and operating system updates to your devices. Employee education, best practices, and overall device security are all part of a sound vulnerability management strategy.

Why it's important

While a solid update strategy will help circumvent many vulnerabilities, routine vulnerability assessments will go beyond software updates to minimize potential loss. Auditing these practices will ensure that you follow best practices and stay on top of current threats.

Questions to ask when auditing vulnerability management practices

- [ ] Do we conduct regular vulnerability assessments on our devices?
- [ ] Is there a process for addressing identified vulnerabilities?
- [ ] Are employees regularly educated on potential threats and best practices for device security?

09

Change Management

Change management ensures practices and procedures are in place to properly approve, execute, and document changes made to devices. Risk assessments should be part of any formal change management process.

Why it's important

Processes around change management are multifold. They ensure a single person isn't making the decision to push changes through, verify that those changes are thoroughly vetted, and enforce proper documentation in case something goes wrong.

Questions to ask when auditing change mangement practices

- [ ] Do we have a formal change management process?
- [ ] Who authorizes and approves changes?
- [ ] Is there a test environment used to assess changes for potential risks?

10

Documentation

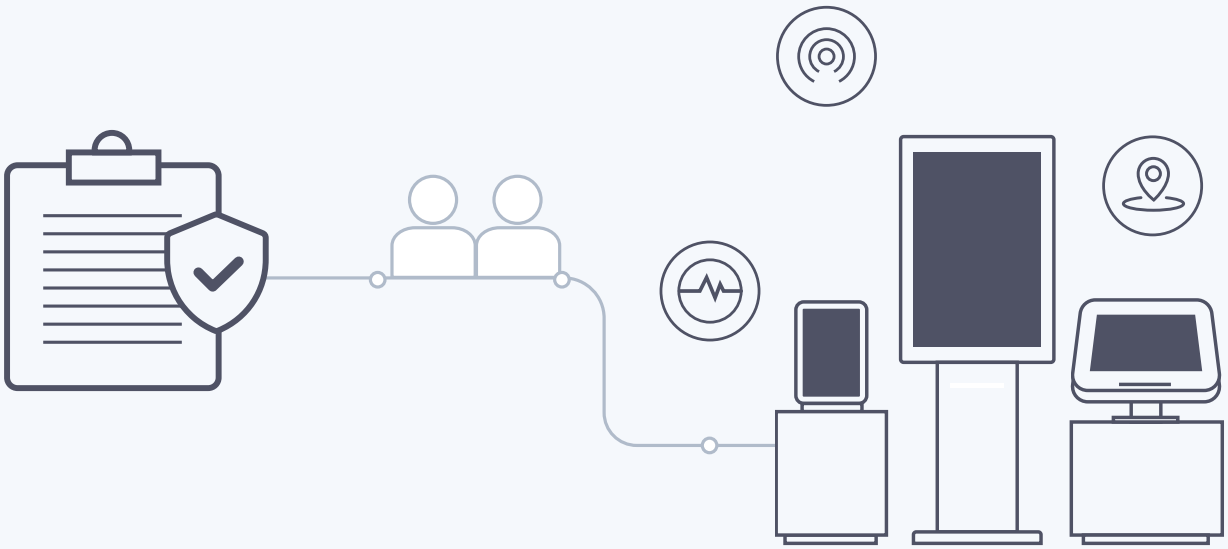
Proper documentation procedures ensure all aspects of your device fleet are well tracked. This audit should also look at policy enforcement to verify employees know and follow documentation practices.

Why it's important

Documentation doesn't start and end with change management — it should cover everything from proper provisioning and deployment practices to troubleshooting, updating, and beyond. Tracking anything that affects your devices will allow you to have a consistent record of what's happening with your fleet.

Questions to ask when auditing documentation practices

- [ ] Do we have thorough documentation policies in place for our devices?
- [ ] Are our current policies and procedures up to date?
- [ ] Are employees adequately trained on documentation policies? Are these policies enforced?



Good IT practices start with awareness of the potential issues. Regularly auditing processes and procedures allows current practices to be evaluated for effectiveness and efficiency while doubling down on best practices and proper documentation. This list is meant to be a jumping-off point that can be expanded upon for your organization.

Esper is the partner you need when it comes to dedicated device management, best practices, device security, paths to upgradability, and more. Our robust device infrastructure was built from the ground up for dedicated devices, while our intuitive console is optimized for usability. What does that mean for you? Maximized device deployment and usage with minimal distractions.

As you work through this guide, if you find that your current device management strategy is lacking, give us a chat — we're ready when you are.

Connect with an expert

Complete Checklist

Configuration Management

- [ ] Is our configuration process well documented and easy to follow?
- [ ] Do our processes align with industry best practices?
- [ ] Is the experience consistent across all devices?

Access Controls

- [ ] Do all these employees need the access they have?
- [ ] Can we offer more granular access control options?
- [ ] Do we have a password reset or multi-factor authentication policy in place? Should we update or change it?

Update Practices

- [ ] Do we have a repeatable, scalable system for delivering app updates? What about system updates and security patches?
- [ ] Do we release regular security patches to our apps and devices in compliance with best practices?
- [ ] Is this process documented?

Physical Security

- [ ] Do we have physical security in place to prevent easy theft? Can our devices be tethered or locked to a single location?
- [ ] Do we have digital tracking to locate devices if they go missing?
- [ ] Are our extra or unused assets securely stored in a locked location? Who has access to this area?

Disaster Recovery

- [ ] Is there a documented backup plan for an internet or other device outage?
- [ ] Has this backup plan been battle tested? Is it effective, or does it need to be updated?
- [ ] Do we have a seamless plan to recover or replace devices quickly if one goes down?

Monitoring and logging

- [ ] Are we tracking essential device stats and logging those in a way that's accessible?
- [ ] Are there metrics or system statistics that we're not monitoring and should be to maximize device health?
- [ ] Do we have the capability to set up automated notifications when a device deviates from the baseline?

Data Backup

- [ ] Is our backup strategy current? Could it be improved?
- [ ] What data are we backing up? Is there anything that can be added?
- [ ] Are our backups air-gapped and redundant if something happens to the current backup sets?

Vulverability management

- [ ] Do we conduct regular vulnerability assessments on our devices?
- [ ] Is there a process for addressing identified vulnerabilities?
- [ ] Are employees regularly educated on potential threats and best practices for device security?

Change Management

- [ ] Do we have a formal change management process?
- [ ] Who authorizes and approves changes?
- [ ] Is there a test environment used to assess changes for potential risks?

Documentation and Policies

- [ ] Do we have thorough documentation policies in place for our devices?
- [ ] Are our current policies and procedures up to date?
- [ ] Are employees adequately trained on documentation policies? Are these policies enforced?