In recent years, mobile devices have found an irresistible presence in the corporate world. The widespread adoption of mobile devices in enterprises got a boost with the COVID-led remote working trend gaining traction. Employees' move to mobile technology has transformed how organisations function, resulting in improved workflows, communications, flexibility, mobility, and efficiency.

Real-time data access and collaboration enabled by mobile devices have jacked up teamwork. With smartphones, tablets, laptops, and even wearables becoming an integral part of most organisations, it's essential to weigh the trade-off in terms of risks. Because enterprise mobile devices access sensitive business data, they can threaten security if it's lost, hacked, or stolen.

These endpoints can work as entry points for black hat artists and can potentially compromise the entire IT infrastructure if adequate security measures are not in place. If sensitive business data is compromised, organisations also risk scrutiny of data protection regulations, which mandate strict protocols for safeguarding personal information.

That's where mobile device management (MDM) steps in as a critical saviour of organisational data. As the landscape of security threats and regulatory enforcement has evolved, IT and security leaders are now tasked with provisioning, managing, and securing mobile devices within their corporate environments. MDM, essentially, controls and secures a wide variety of mobile devices used in the workplace.

What is mobile device management (MDM)?

Mobile device management is a set of software solutions and strategies, including on-device applications and configurations, corporate policies, and backend infrastructure. It allows IT to automate, secure, and enforce policies on mobile devices connected to an organisation's network, simplifying the IT management of end user devices.

The roots of MDM go back to the early 2000s, when the first wave of mobile devices, especially the launch of Apple's first iPhone in 2007, hit the enterprise realm. The recent Bring Your Own Device (BYOD) trend that has left organisations vulnerable to issues with shadow IT has further snowballed the importance of mobile device management.

Key features and components of mobile device management

- Device monitoring: In an MDM programme, dedicated work devices are assigned to each employee. These devices have an MDM agent installed that connects them directly with the MDM server. The MDM server collects a host of data about devices, including real-time GPS location, usage statistics, malware detection, and compliance with organisational and industry policies.
  Every time an unauthorised access is attempted, unapproved applications are installed, or policies are violated, the MDM agent triggers an alert to notify IT administrators. Device monitoring also gets useful in emergencies when an employee loses a device and needs help recovering it.
- Policy enforcement: An effective MDM solution enables administrators to set rules that coincide with their organisational objectives. These rules, as part of policy enforcement, ensure that mobile devices that are part of organisational assets or have access to sensitive data adhere to corporate policies.
  These policies include management of applications, networks, and content; implementation of security measures such as password policies, remote wipes, and lock functionalities; provision of access controls as per roles and responsibilities; and monitoring and reporting of compliance.
- Software distribution: The MDM software distribution feature allows administrators to remotely deploy, update, and manage applications on mobile devices. MDM allows integration with both app stores, like the Apple App Store and Google Play Store, and enterprise app stores for seamless app distribution and updates.
  As the policy allows, admins can remotely push the applications to install on managed devices, either with user consent or without their intervention. It ensures all applications across managed devices are

running updated versions of applications, and if need be, they could be rolled back to the previous version.

Basics of ISO 27001

In this digital age, where data is the new currency, its privacy and security are top priorities for organisations worldwide. If an organisation's ISMS is compromised, it risks losing valuable information assets, which can result in reputational and financial damages.

To organisations' rescue, the internationally recognised ISO 27001 framework provides a robust framework for the information security risk management process. It thereby helps organisations minimise the security gaps that could lead to unauthorised access, disclosure, alteration, or destruction of sensitive information.

ISO 27001 is an international standard for information security management published by the ISO in collaboration with the IEC, leading international organisations that develop international standards. It provides a framework for requirements for defining, implementing, operating, and improving an organisation's information security management system (ISMS).

Compliance with ISO 27001 demonstrates the organisation's commitment to information security. ISO 27001 certification eases companies' compliance with data protection regulations like the GDPR, gives them a competitive edge in the international marketplace, and makes them trusted by clients and stakeholders.

Main components and structures of the standard

As a member of the ISO 27000 series, ISO 27001 is the most commonly certified standard. Its popularity and effectiveness have led to many organisations adopting it for their IT governance, risk management, and compliance programmes. Compliance with ISO 27001, and therefore maintaining a strong ISMS, requires a structured approach. One such approach is the Plan-Do-Check-Act (PDCA) cycle.

- Plan: Laying the foundation
  The plan phase begins with setting clear objectives for ISMS, which

should be in alignment with the organisation's strategic goals. Objectives for organisations can vary depending on whether they're aiming to comply with regulatory requirements, protect sensitive data, or improve their overall cybersecurity posture.
This step involves conducting a comprehensive risk assessment of the ISMS. It helps organisations identify threats and vulnerabilities unique to them in terms of system characteristics, management, complexity, people, technology in place, etc. It thereby lays the foundation for selecting and implementing the appropriate security controls as mentioned under the ISO 27001 framework.

- Do: Turning plans into action
  The Do phase involves developing and enforcing ISMS policies, deploying security software, and providing training to employees. It requires organisations to conduct risk assessments and evaluate the reasons behind each structure. This phase includes the preparation of procedures that address identified risks and the implementation of appropriate security controls.
- Check: Continuous monitoring and review
  Maintaining optimal performance is a must to ensure the results of processes are within the expected range. This phase covers monitoring, measuring, analysis, and evaluation checks of the implemented controls against the defined policies and objectives. Continuous monitoring of the key performance indicators (KPIs) provides valuable insights into the health of the ISMS and helps identify, treat, eliminate, or improve the detected issues.
- Act: Updates and improvements to the ISMS
  The final phase in the PDCA cycle, Act, is about taking corrective actions based on findings from the Check phase to achieve continual improvement of the ISMS. Insights derived from the Check phase may require organisations to do some man-hours or even redesign the existing system (in the worst cases). Based on risk assessment, organisations can prioritise which gaps to tackle immediately and which ones to hold for later. The PDCA cycle is a close loop activity that requires dynamic improvement over time.

Connection between MDM and ISO 27001

As threats became more sophisticated, ISO/IEC released a new version of ISO 27001 in 2022, reflecting the need to secure mobile devices and form policies around their use. Mobile device management (MDM) best practices effectively address the following controls outlined in Annex A of ISO 27001:2022.

Information security policies (Clause 5.2)

Clause 5.2 of ISO 27001 requires top management in an organisation to establish an information security policy. It's one of the first documents an organisation needs to create when building their ISMS. This policy communicates the purposes and impact of information security to all staff members. When formally communicated, the policy provides a clear vision and direction, helping everyone to understand the organisation's objectives and strategic approach to information security.

MDM solutions allow organisations to draft policies related to security, such as mandatory encryption, password policies, access controls, etc. These policies are applied across all mobile devices, ensuring they comply with the organisation's security standards. MDM provides a centralised view of all devices' performances and monitors compliance with corporate policies.

It enables organisations to manage security settings across all mobile devices from a single platform and enforce secure configurations on devices of concern. Push notification features on MDM platforms allow organisations to directly manage updates of software on user devices and convey any information as a notification that could be important for users' following best practices.

Access Controls (Clause 9)

Compliance with the ISO 27001 standard requires meeting 14 access controls as detailed in control category A.9. It may be daunting, but thanks to mobile device management, it checks all the boxes pretty well.

Annex 9 focuses on four key areas and how MDM addresses each:

- Policy: Annex A.9.1 requires creating policies on access controls, documenting these policies, defining roles and responsibilities for access rights, and detailing how the organisation manages them. MDM solutions empower organisations to formulate and enable policies related to

application management, content control, and access rights management, effectively meeting policy requirements.

- Access: Annex A.9.2 requires managing and reviewing access rights, including user provisioning, authorisation, and restriction. By implementing robust authentication protocols and access controls, MDM solutions ensure that only the right people with authority can access the sensitive information stored on mobile devices.
- User responsibilities: Annex A.9.3 requires making sure users understand the organisation's security requirements and follow good access control practices. MDM platforms provide users with education on security requirements and guidelines, promoting user responsibilities and awareness about access rights.
- Unauthorised access prevention: Annex A.9.5 requires securing access to systems and applications to prevent bad guys from getting access to sensitive information. Mechanisms like information access restrictions, secure log-on, password management, and source code access, which are covered under Annex A.9.4, are also implemented by MDM platforms, satisfying the requirements of ISO 27001.

Cryptography (Clause 10)

Annex A.10.1 is about cryptographic controls. Its objective is to put effective cryptographic and encryption controls in place to ensure the confidentiality, authenticity, and integrity of business information. Policy creation on the use of encryption helps identify business requirements where encryption can be vital to implement.

It's important to select the right cryptographic technologies and techniques; otherwise, poor choice and management of cryptographic materials (e.g., keys and certificates) can themselves lead to vulnerabilities in the system. Often, the management of key materials (Annex A.10.2) is the weakest point, so having robust and secure processes around them, from their creation, distribution, changes, backup, and storage to their destruction, is crucial in maintaining the security of the system.

MDM enables organisations to enforce encryption on mobile devices. It includes the compulsory encryption of data at rest and in transit, as well as configuring devices with organisation-approved cryptographic standards. A good MDM

solution provides configuration options for FileVault, which encrypts the entire contents of a Mac's hard drive using encryption methods like XTS-AES-128.

Secure management of cryptographic keys ensures controlled generation, distribution, and storage. With the escrowing key feature, even if the primary key is lost or forgotten, it is possible to decrypt data with the recovery key available.

Deeploi.io as an MDM integration for ISO 27001

At Kertos, we help companies transform data protection into actual compliance. No matter the amount of data or complexity within an organisation's privacy processes, Kertos.io always delivers. Our ISO 27001 software comprises various tools and mechanisms that make your ISMS management and enhancement as easy as pie.

To make your company ISO 27001-compliant, we're equipped with the best tools in our arsenal. Only the MDM integration missing so far has been achieved with our partnership with Deeploi.io, which boosts our ISO 27001 certification capabilities.

The comprehensive MDM capabilities offered by Deeploi enable organisations to enforce security policies in line with ISO 27001 requirements across all mobile devices. With the best encryption techniques, it ensures that your sensitive information data is protected as per ISO 27001 standards, whether at rest or in transit. For more information on how we can help you with MDM integration for ISO 27001 compliance, contact us today.