Core ISO/IEC 27000 Family Standards

The **ISO/IEC 27000 family of standards**, developed by the **International Organization for Standardization (ISO)** and the **International Electrotechnical Commission (IEC)**, provides a framework for establishing and managing an **Information Security Management System (ISMS)** and related cybersecurity practices. The "core" standards are those foundational to the series, defining the ISMS, its requirements, controls, and supporting processes like risk management, auditing, and monitoring. Below is a list of the **core ISO/IEC 27000 family standards** as of October 2025, based on the latest available information.

Core ISO/IEC 27000 Family Standards

The core standards are essential for organizations implementing or certifying an ISMS, providing the foundation for the entire ISO 27000 series. These are the most widely referenced and critical standards for establishing, implementing, and maintaining information security: (Clarification: 'Core' is an industry convention, not an official ISO designation.)

1. **ISO/IEC 27000:2018** – *Information Security Management Systems – Overview and Vocabulary*
    - Provides an introduction to the ISO 27000 family, defining key terms, concepts, and principles used across the series.
    - Outlines the purpose, structure, and scope of an ISMS.
    - Essential for understanding the terminology and framework of the series.
2. **ISO/IEC 27001:2022** – *Information Security Management Systems – Requirements*
    - The certifiable standard specifying requirements for establishing, implementing, maintaining, and improving an ISMS.
    - Includes 93 controls in **Annex A** (aligned with ISO 27002:2022) across four domains: organizational, people, physical, and technological.
    - Basis for third-party audits and certification, widely adopted across industries (e.g., tech, healthcare, finance).
3. **ISO/IEC 27002:2022** – *Information Security Controls*
    - Provides detailed implementation guidelines for the 93 controls listed in ISO 27001's Annex A.

- Covers controls such as access management, encryption, incident response, and supplier relationships.
- Serves as a practical guide for organizations to select and apply controls based on risk assessments.

4. **ISO/IEC 27003:2017** – *Information Security Management Systems – Guidance*
   - Offers practical guidance for implementing an ISMS as per ISO 27001.
   - Covers defining scope, conducting risk assessments, selecting controls, and managing the ISMS lifecycle.
5. **ISO/IEC 27004:2016** – *Information Security Management – Monitoring, Measurement, Analysis, and Evaluation*
   - Provides guidelines for monitoring and measuring the effectiveness of an ISMS.
   - Includes metrics, performance indicators, and evaluation methods to ensure controls meet objectives.
6. **ISO/IEC 27005:2022** – *Information Security Risk Management*
   - Provides a structured approach to identifying, assessing, and treating information security risks within an ISMS.
   - Aligns with ISO 31000 (general risk management) and supports ISO 27001's risk-based approach.
7. **ISO/IEC 27006:2024** – Requirements for Bodies Providing Audit and Certification of Information Security Management Systems (Note: This version may not be officially released; verify with ISO for confirmation.)
   - Specifies requirements for accreditation bodies and auditors conducting ISO 27001 certification audits.
   - Ensures consistency and competence in ISMS certification processes.
8. **ISO/IEC 27007:2020** – *Guidelines for Information Security Management Systems Auditing*
   - Provides detailed procedures for conducting internal and external ISMS audits to verify ISO 27001 compliance.
   - Focuses on audit planning, execution, and reporting.

Note:

- These eight standards are considered "core" because they directly support the establishment, certification, and maintenance of an ISMS, forming the backbone of the ISO 27000 series.
- Other standards in the series (e.g., ISO 27017 for cloud security, ISO 27701 for privacy) are specialized and not typically classified as core, though they may be critical for specific contexts.
- Standards are periodically revised; the versions listed (e.g., 27001:2022) reflect the latest as of October 2025. New revisions or standards may emerge post-2025.

Informational Resources

- **ISO Official Website**: iso.org/isoiec-27001-information-security.html (overview, purchase standards, FAQs).
- **ISO/IEC 27000:2018**: iso.org/standard/73906.html (free preview, paid full text).
- **ISO/IEC 27001:2022**: iso.org/standard/27001 (certifiable standard, paid).
- **ISO/IEC 27002:2022**: iso.org/standard/27002 (control guidelines, paid).
- **Training and Tools**:
    - ISO Training Partners: iso.org/training (list of accredited providers).
    - ISACA ISO 27001 Training: isaca.org/training-and-events/iso-27001 (paid certifications, e.g., CISM).
    - Advisera 27001 Toolkit: advisera.com/27001academy (free templates, paid ISMS software).
    - BSI Training: bsigroup.com/en-US/ISO-27001/training (paid courses, toolkits).
- **Industry Resources**:
    - “ISO 27000 Series Guide” (free PDFs from vendors like Secureframe, Vanta).
    - IT Governance: itgovernanceusa.com/iso-27001 (checklists, toolkits).
- **Community Support**:
    - ISACA Cybersecurity Community: isaca.org/connect (ISO 27000 forums, events).
    - ISO Community: iso.org/communities (discussion groups, webinars).

If you need details on a specific core standard (e.g., ISO 27005 for risk management) or guidance on implementing these standards, let me know your next steps!