EMBA Program
MB-551

Cybersecurity Agencies & Standards
International & India

Several international standards exist to guide and establish best practices in cybersecurity. These standards are developed by various organizations to address different aspects of cybersecurity. Some prominent international standards include:

1. ISO/IEC 27001: Information Security Management System (ISMS):

- Developed by: International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC)

- Focus: Establishes the criteria for an information security management system, providing a systematic approach to managing sensitive company information.

2. ISO/IEC 27002: Code of Practice for Information Security Controls:

- Developed by: ISO and IEC

- Focus: Provides guidelines for organizational information security standards and information security management practices.

3. NIST SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations:

- Developed by: National Institute of Standards and Technology (NIST) in the United States

- Focus: Offers a comprehensive catalog of security and privacy controls for information systems.

4. NIST Cybersecurity Framework:

- Developed by: NIST

- Focus: Outlines a framework that organizations can adopt to manage and improve their cybersecurity risk management processes.

5. GDPR (General Data Protection Regulation):

- Developed by: European Union (EU)

- Focus: Specifies regulations for the protection of personal data and privacy of individuals within the EU, impacting how organizations handle and process such data.

6. PCI DSS (Payment Card Industry Data Security Standard):

- Developed by: Payment Card Industry Security Standards Council (PCI SSC)

- Focus: Establishes security requirements for organizations that handle credit card transactions, ensuring the protection of cardholder data.

7. CIS Critical Security Controls:

- Developed by: Center for Internet Security (CIS)

- Focus: Provides a set of prioritized actions to protect organizations and data from common cyber threats.

8. IETF RFCs (Internet Engineering Task Force Request for Comments):

- Developed by: Internet Engineering Task Force (IETF)

- Focus: A series of publications that define various aspects of internet standards, protocols, and related issues, including security considerations.

9. ITIL (Information Technology Infrastructure Library):

- Developed by: AXELOS

- Focus: Offers a set of practices for IT service management, including guidance on cybersecurity management within an IT environment.

10. Cybersecurity Act of the European Union:

- Developed by: European Union Agency for Cybersecurity (ENISA)

- Focus: Establishes a framework for the certification of cybersecurity products and services within the European Union.

Organizations often use a combination of these standards based on their industry, regulatory requirements, and the nature of their digital assets to create a robust cybersecurity posture. Compliance with these standards enhances cybersecurity resilience and demonstrates a commitment to protecting information and systems on an international scale.

India has been actively working on strengthening its cybersecurity framework, and several standards and guidelines have been established to address cybersecurity concerns. Please note that developments may have occurred since then, and it's advisable to check for the latest information. Here are some key cybersecurity standards and initiatives in India:

1. Information Technology (IT) Act, 2000:

- The IT Act provides the legal framework for electronic governance and cybersecurity in India. It addresses issues related to unauthorized access, data protection, and computer-related offenses.

2. National Cyber Security Policy, 2013:

- This policy outlines the strategic vision and objectives to enhance cybersecurity in India. It emphasizes the protection of information and infrastructure, along with the development of a secure cyberspace environment.

3. Indian Computer Emergency Response Team (CERT-In):

- CERT-In is the national agency responsible for responding to cybersecurity incidents. It provides guidelines, advisories, and best practices for securing information systems.

4. ISO/IEC 27001:

- While not specific to India, ISO/IEC 27001 is an international standard for information security management systems. Many Indian organizations adopt this standard to enhance their cybersecurity posture.

5. Data Security Council of India (DSCI):

- DSCI is a premier organization dedicated to promoting data protection and cybersecurity. It offers various frameworks, including the DSCI Security Framework (DSF), to help organizations implement effective cybersecurity practices.

6. Reserve Bank of India (RBI) Guidelines:

- RBI issues guidelines for the cybersecurity framework in the banking and financial sector. These guidelines outline measures to be adopted by financial institutions to secure customer data and financial transactions.

7. National Critical Information Infrastructure Protection Centre (NCIIPC):

- NCIIPC focuses on protecting critical information infrastructure in sectors such as energy, transportation, and finance. It plays a vital role in enhancing the cybersecurity posture of critical sectors.

8. Telecom Regulatory Authority of India (TRAI) Recommendations:

- TRAI issues recommendations to telecom service providers to ensure the security and integrity of communication networks. This includes guidelines for securing customer data and preventing unauthorized access.

9. Bureau of Indian Standards (BIS):

- BIS develops standards for various sectors, and while it may not have specific cybersecurity standards, it contributes to overall quality and security standards that indirectly impact cybersecurity.

10. Indian Cyber Crime Coordination Centre (I4C):

- I4C is established to combat cybercrime and enhance cybersecurity. It works on issues related to cyber threats, law enforcement, and coordination among various stakeholders.

It's crucial for organizations in India to stay updated on the latest cybersecurity standards and guidelines issued by relevant authorities to ensure compliance and resilience against evolving cyber threats. Additionally, the government continues to work on strengthening the cybersecurity landscape, and new initiatives may have been introduced since my last update.