Lanka Education And Research Network

Security Standards, Regulations, Consequences and law

LkNOG

Cyber Security Standards

- Cyber security standards are collections of best practices created by experts to protect organizations from cyber threats and help improve their cyber security posture.

- Cyber security frameworks are generally applicable to all organizations, regardless of their size, industry, or sector.

ISO/IEC 27001:2013 Information technology

Security techniques — Information security management systems — Requirements

ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature.

The following context shows some minor legislation of cyber security:

- UK specific laws and policies, e.g. Electronic Communications Act (**2000**)
- Electronic Signatures Regulations (**2002**)
- Wassenaar Arrangement (**1996**)
- Regulation of Investigatory Powers Act (**2016**)
- International Traffic in Arms Regulations (ITAR), disclosure laws, e.g. Public Interest Disclosure Act (**1998**)
- Freedom of Information Act (**2000**)
- Data Protection Act (**2018**)
- General Data Protection Regulation (GDPR) (**2016**)
- Computer Misuse Act (**1990**), The Serious Crime Act (**2015**), Police and Justice Act (**2006**)

Encryption Standard

Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) is a symmetric block cipher chosen by the U.S. government to protect classified information.

AES is implemented in software and hardware throughout the world to encrypt sensitive data. It is essential for government computer security, cyber security, and electronic data protection.

The National Institute of Standards and Technology (NIST) started the development of AES in 1997 when it announced the need for an alternative to the Data Encryption Standard (DES), which was starting to become vulnerable to brute-force attacks.

Encryption Standard

NIST stated that the newer, advanced encryption algorithm would be unclassified and must be "capable of protecting sensitive government information well into the [21st] century." It was intended to be easy to implement in hardware and software, as well as in restricted environments -- such as a smart card -- and offer decent defenses against various attack techniques.

AES was created for the U.S. government with additional voluntary, free use in public or private, commercial or noncommercial programs that provide encryption services. However, non-governmental organizations choosing to use AES are subject to limitations created by U.S. export control.

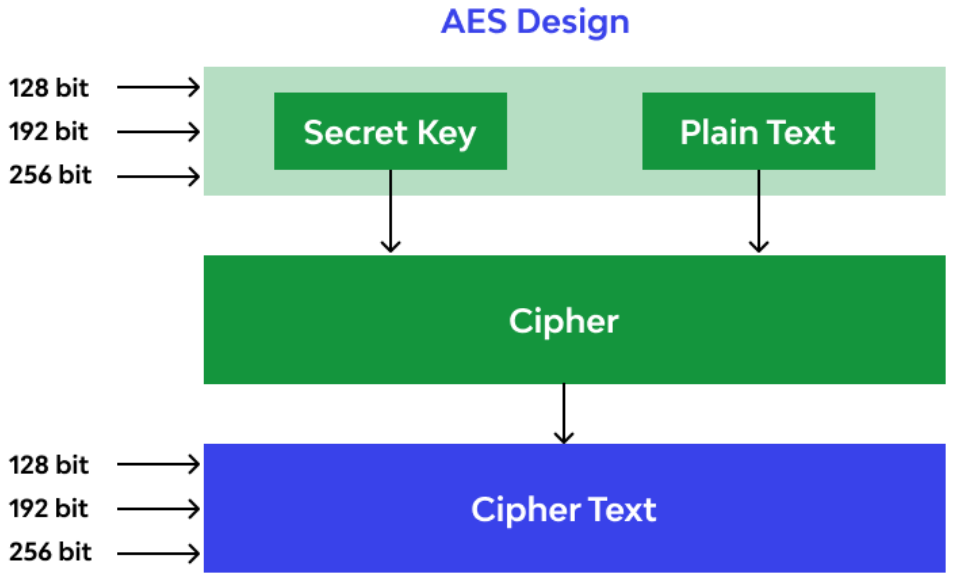
How AES encryption works?

AES includes three block ciphers:

- AES-128 uses a 128-bit key length to encrypt and decrypt a block of messages.
- AES-192 uses a 192-bit key length to encrypt and decrypt a block of messages.
- AES-256 uses a 256-bit key length to encrypt and decrypt a block of messages.

Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128, 192 and 256 bits, respectively.

Symmetric, also known as secret key, ciphers use the same key for encrypting and decrypting. The sender and the receiver must both know -- and use -- the same secret key.



What are the features of AES?

- NIST specified the new AES algorithm must be a block cipher capable of handling 128-bit blocks, using keys sized at 128, 192 and 256 bits.
- Other criteria for being chosen as the next AES algorithm included the following:
- Security. Competing algorithms were to be judged on their ability to resist attack as compared to other submitted ciphers. Security strength was to be considered the most important factor in the competition.
- Cost. Intended to be released on a global, nonexclusive and royalty-free basis, the candidate algorithms were to be evaluated on computational and memory efficiency.
- Implementation. Factors to be considered included the algorithm's flexibility, suitability for hardware or software implementation, and overall simplicity.

RSA Encryption

- RSA encryption is a public-key encryption technology developed by RSA Data Security. The RSA algorithm is based on the difficulty in factoring very large numbers. Based on this principle, the RSA encryption algorithm uses prime factorization as the trap door for encryption. Deducing an RSA key, therefore, takes a huge amount of time and processing power. RSA is the standard encryption method for important data, especially data that's transmitted over the Internet.

- RSA stands for the creators of the technique, Rivest, Shamir and Adelman.

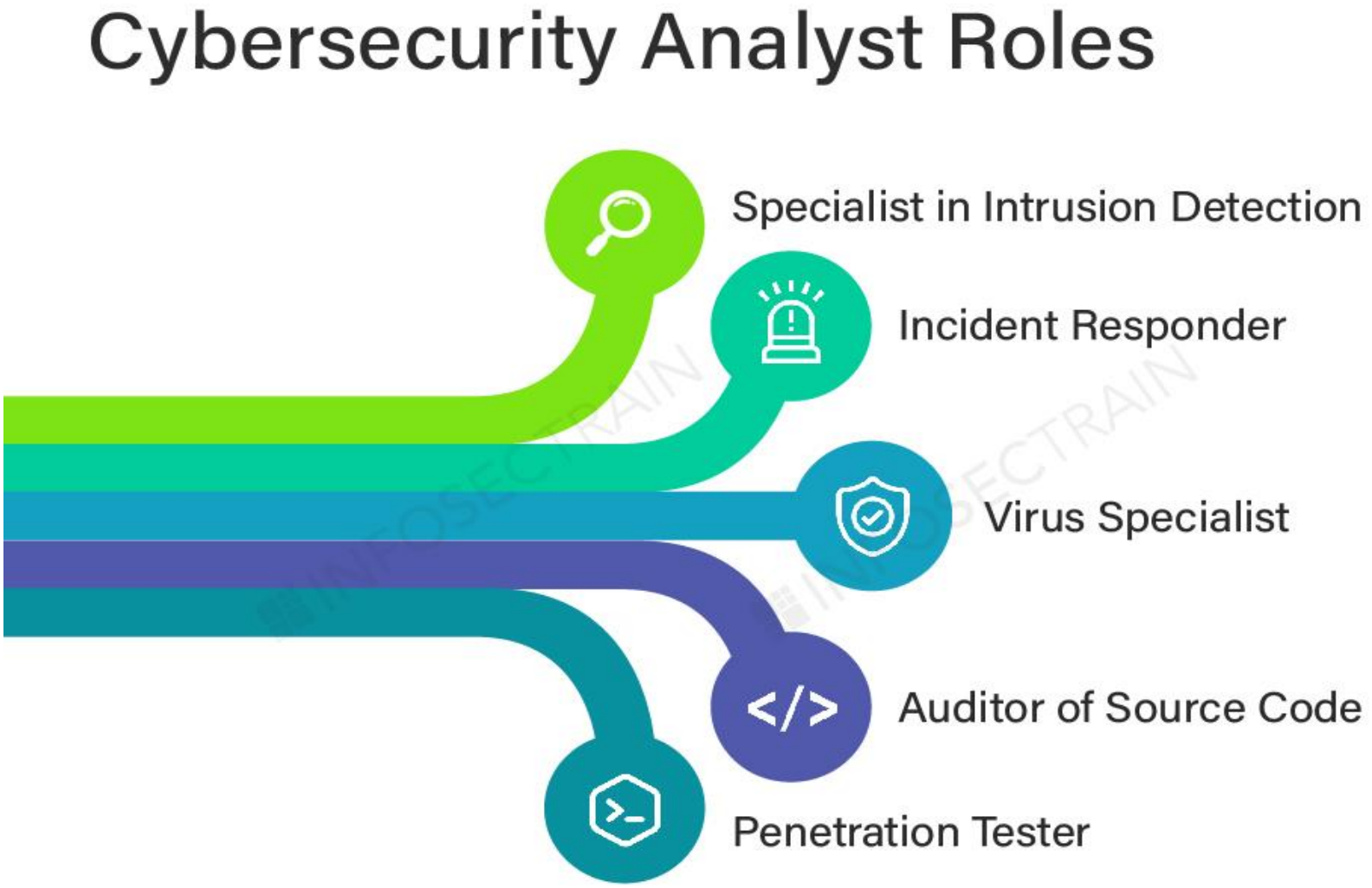
Key Roles in an Incident Response Team

- To execute an incident response plan, you need an incident response team. In a large organization the roles may be carried out by full-time employees or entire teams; in smaller organizations, they can be filled by employees with other full-time roles, who also participate in the incident response process. The following are essential roles within the team.

Key Roles in an Incident Response Team

- **Incident response managers**—have at least two members of staff responsible for approving the incident response plan and coordinating activity when an incident occurs.
- **Security analysts**—review alerts, identify possible incidents and perform an initial investigation to understand the scope of an attack.
- **Threat researchers**—responsible for providing contextual information around a threat, using information from the web, threat intelligence feeds, data from security tools, etc.
- **Other stakeholders**—these can include senior management or board members, HR, PR, and senior security staff such as the Chief Information Security Office (CISO)
- **Third parties**—such as lawyers, outsourced security services, or law enforcement agencies.

Key Roles in an Incident Response Team



NIST Recommendations for Organizing A Computer Security Incident Response Team (CSIRT)

- The NIST Computer Security Incident Handling Guide provides in-depth guidelines on how to build an incident response capability within an organization. It covers several models for incident response teams, how to select the best model, and best practices for operating the team. Incident Response Team Models.

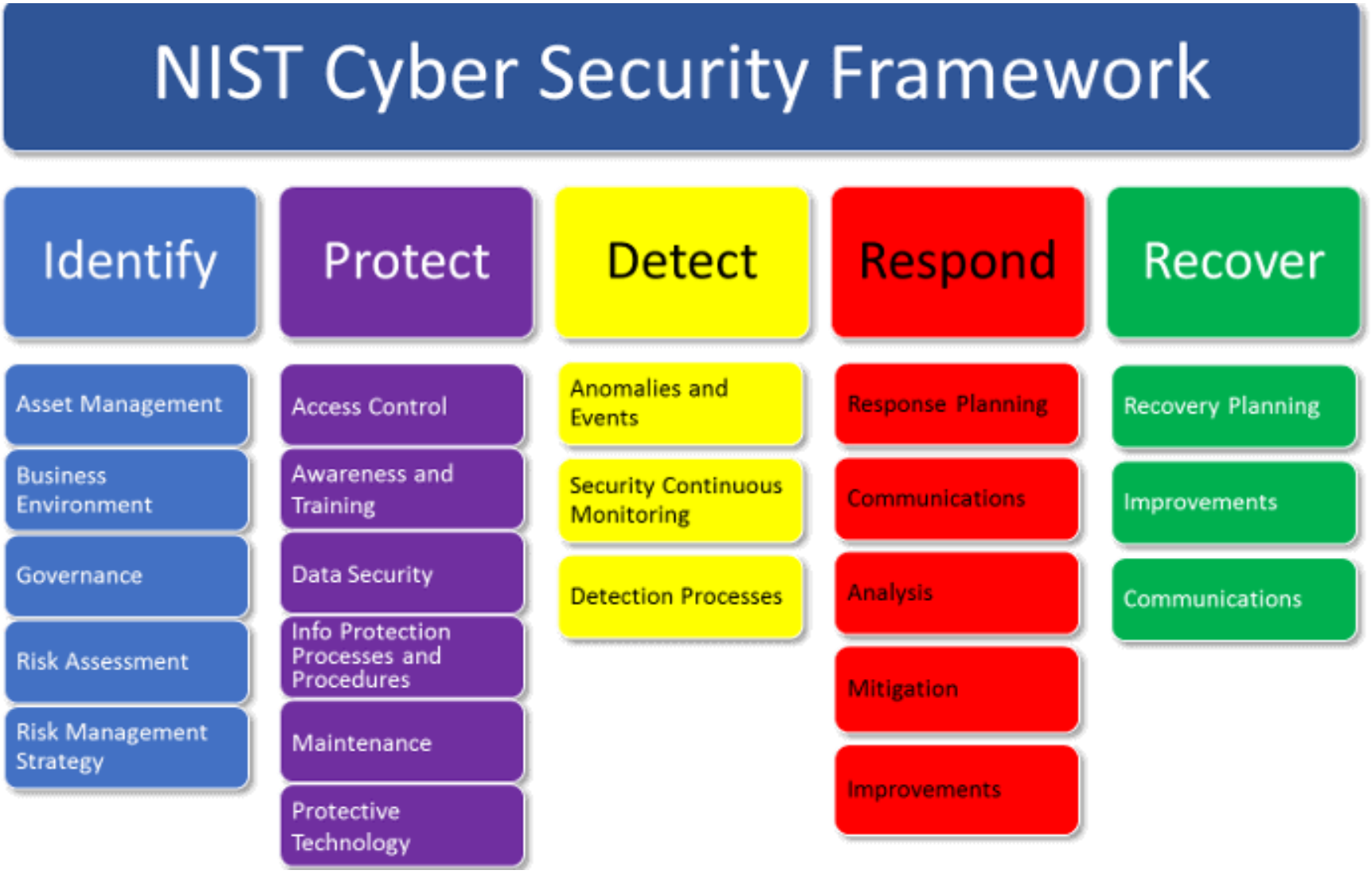
NIST offers three models for incident response teams:

- Central—centralized body that handles incident response for the entire organization.
- Distributed—multiple incident response teams, with each one responsible for a physical location (e.g. branch office), a department or a part of the IT infrastructure
- Coordinated—a central incident response team that works together with distributed incident response teams, without having authority over them. The central team serves as a knowledge center and offers assistance with complex, critical, or organization-wide incidents

What is NIST?

- The National Institute of Standards and Technology is an agency operated by the USA Department of Commerce that provides standards and recommendations for many technology sectors. Within NIST, the Information Technology Laboratory (ITL) is responsible for developing standards and measurement methods for IT, including information security.

What is NIST?


NIST Cyber Security Framework
Identify
Asset Management
Business Environment
Governance
Risk Assessment
Risk Management Strategy
Protect
Access Control
Awareness and Training
Data Security
Info Protection Processes and Procedures
Maintenance
Protective Technology
Detect
Anomalies and Events
Security Continuous Monitoring
Detection Processes
Respond
Response Planning
Communications
Analysis
Mitigation
Improvements
Recover
Recovery Planning
Improvements
Communications

The role of cybercrime law

- Cybercrime law identifies standards of acceptable behavior for information and communication technology (ICT) users; establishes socio-legal sanctions for cybercrime; protects ICT users, in general, and mitigates and/or prevents harm to people, data, systems, services, and infrastructure, in particular; protects human rights; enables the investigation and prosecution of crimes committed online (outside of traditional real-world settings); and facilitates cooperation between countries on cybercrime matters (UNODC, 2013, p. 52).

- Cybercrime law provides rules of conduct and standards of behavior for the use of the Internet, computers, and related digital technologies, and the actions of the public, government, and private organizations; rules of evidence and criminal procedure, and other criminal justice matters in cyberspace; and regulation to reduce risk and/or mitigate the harm done to individuals, organizations, and infrastructure should a cybercrime occur. Accordingly, cybercrime law includes substantive, procedural and preventive law.

Legal systems

Each state has its own legal system, which affects the creation of substantive criminal law on cybercrime. These systems include (Maras, forthcoming, 2020):

1) Common law. These systems create laws by legal precedent(i.e., ruling in case binding to the court and lower courts) and established practice. These laws exist as separate laws and case law (i.e., law that develops from court decisions or legal precedent).

2) Civil law. These legal systems have codified, consolidated, and comprehensive legal rules or statutes that delineate basic rights, responsibilities, duties and expectations of behaviour. These legal systems are primarily based on legislation and constitutions.
3) Customary law. These legal systems include established and accepted patterns of behaviour within a culture that are perceived by those within the culture to be law (opinion juris). In international law, customary law governs relationships and practices between states and is considered binding for all states.

Legal systems

4) Religious law. These legal systems include rules derived from religion or the use of religious documents as a legal source and authority.

5) Legal pluralism. In this type of legal system, two or more of the above-mentioned legal systems (i.e., common, civil, customary or religious law) may exist.

Thank You