RIPHAH INTERNATIONAL UNIVERSITY

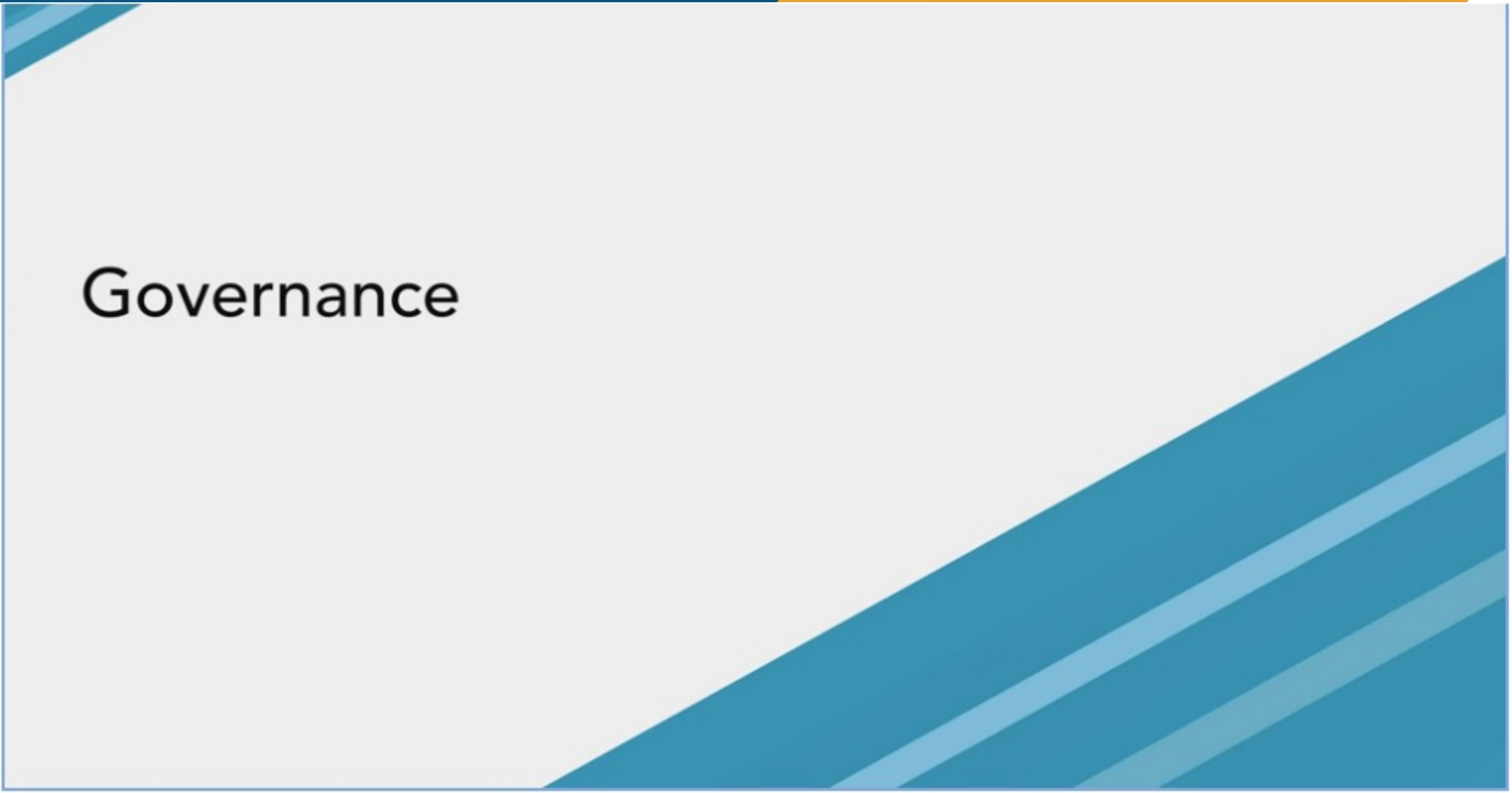
Security Principles-II

Lec09–Information Security

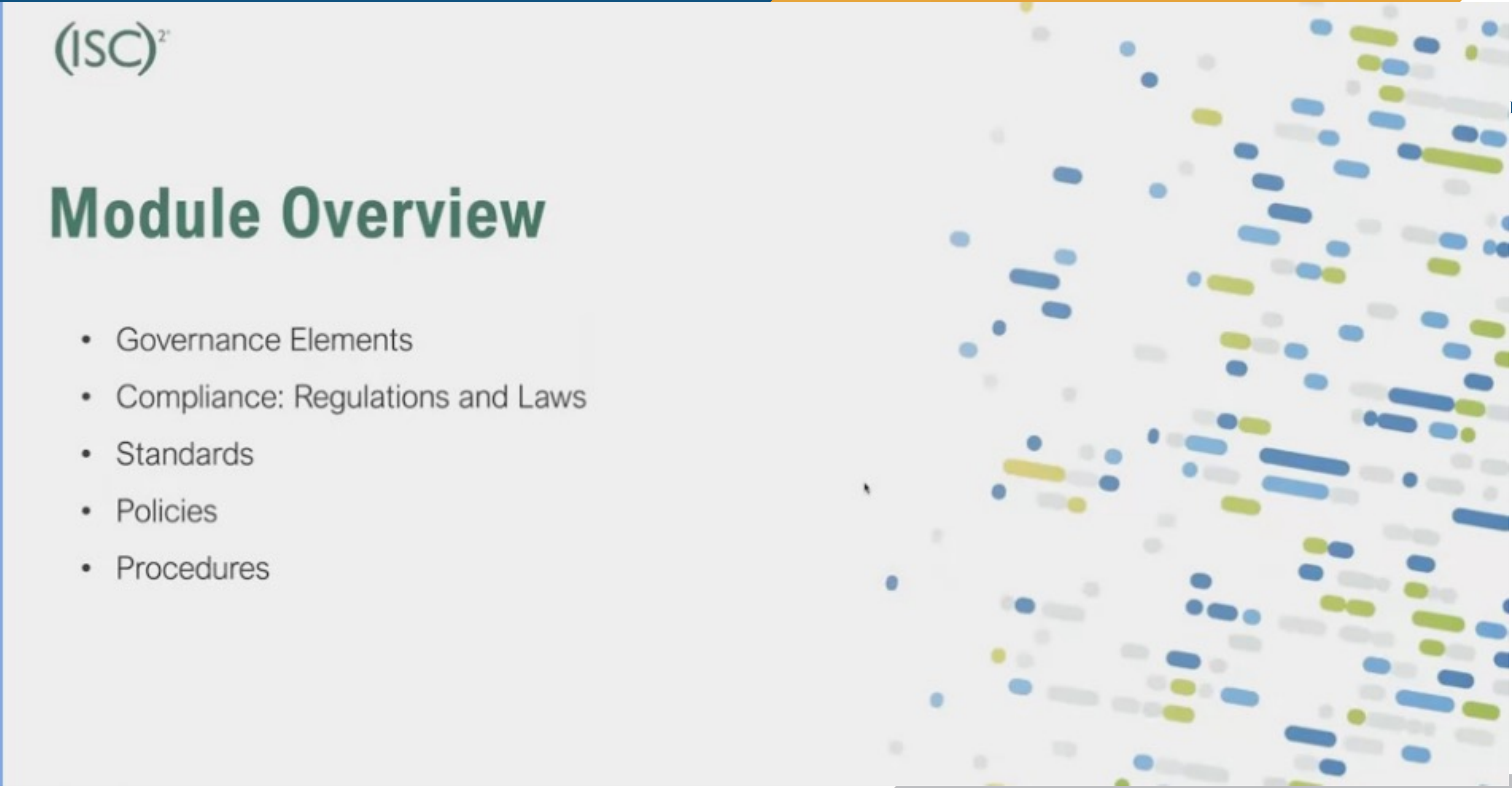
Prepared by
Saadia Aziz

saadia.aziz@riphah.edu.pk

Educate-Enlighten-Empower



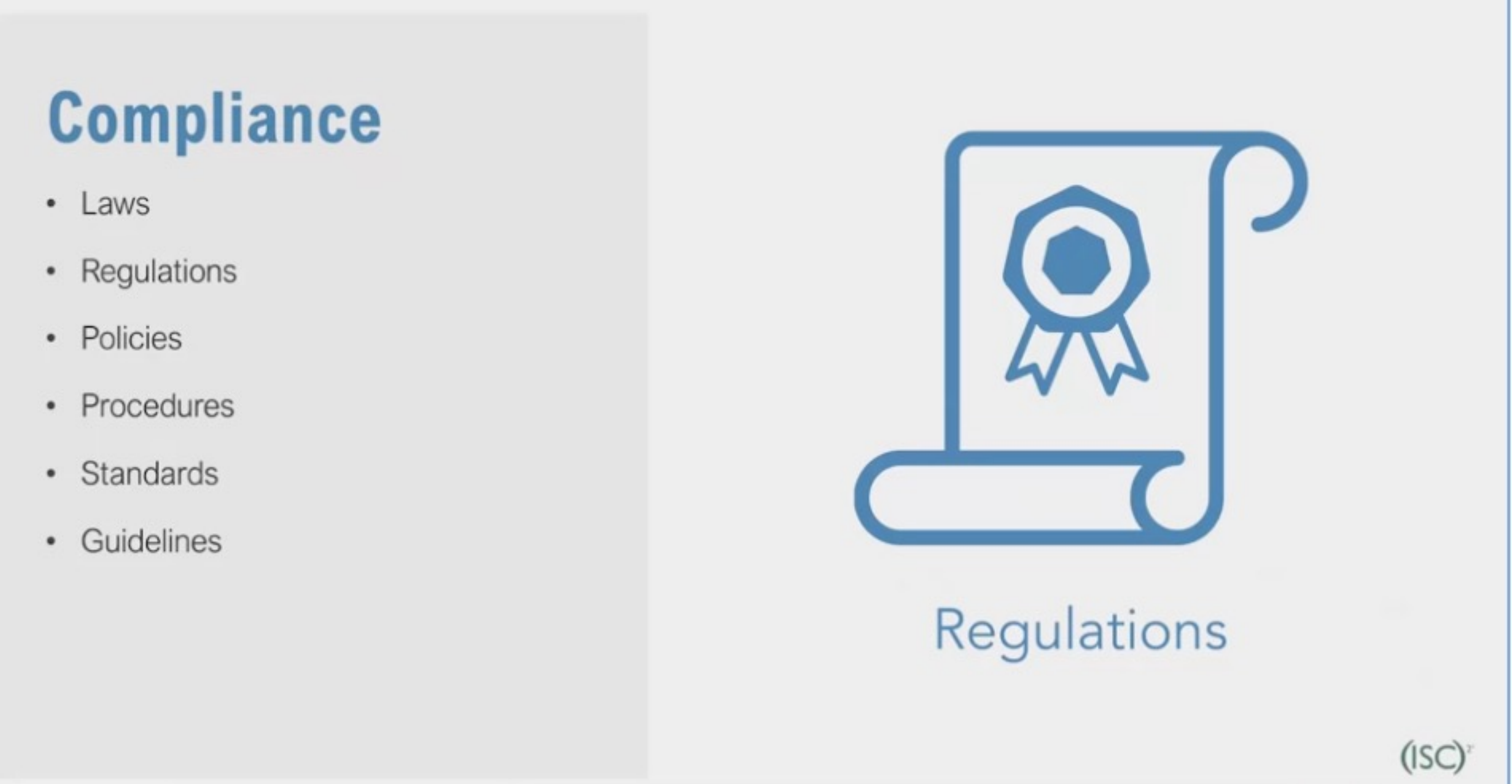
Governance



(ISC)²

Module Overview

- Governance Elements
- Compliance: Regulations and Laws
- Standards
- Policies
- Procedures

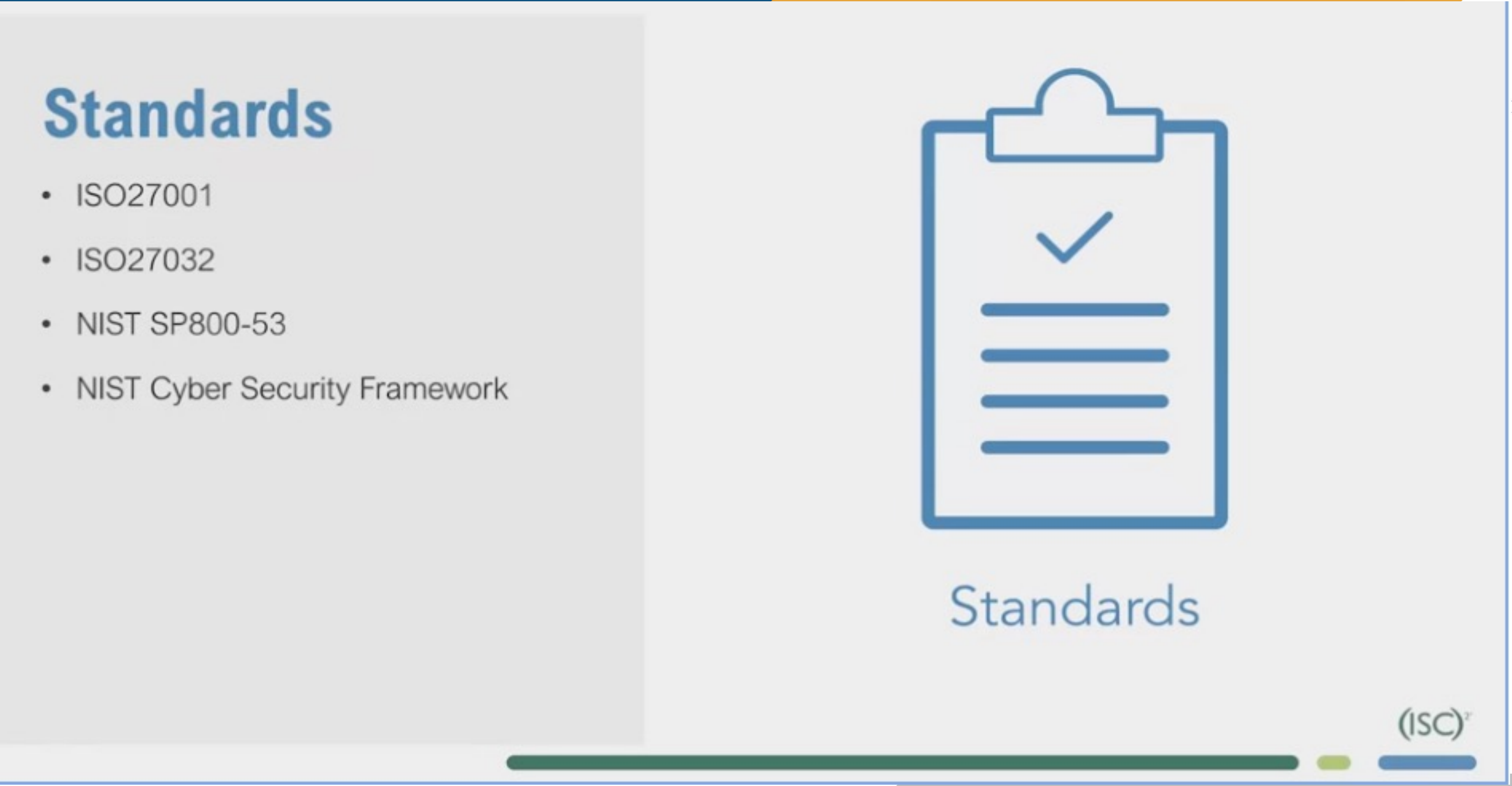


Compliance

- Laws
- Regulations
- Policies
- Procedures
- Standards
- Guidelines

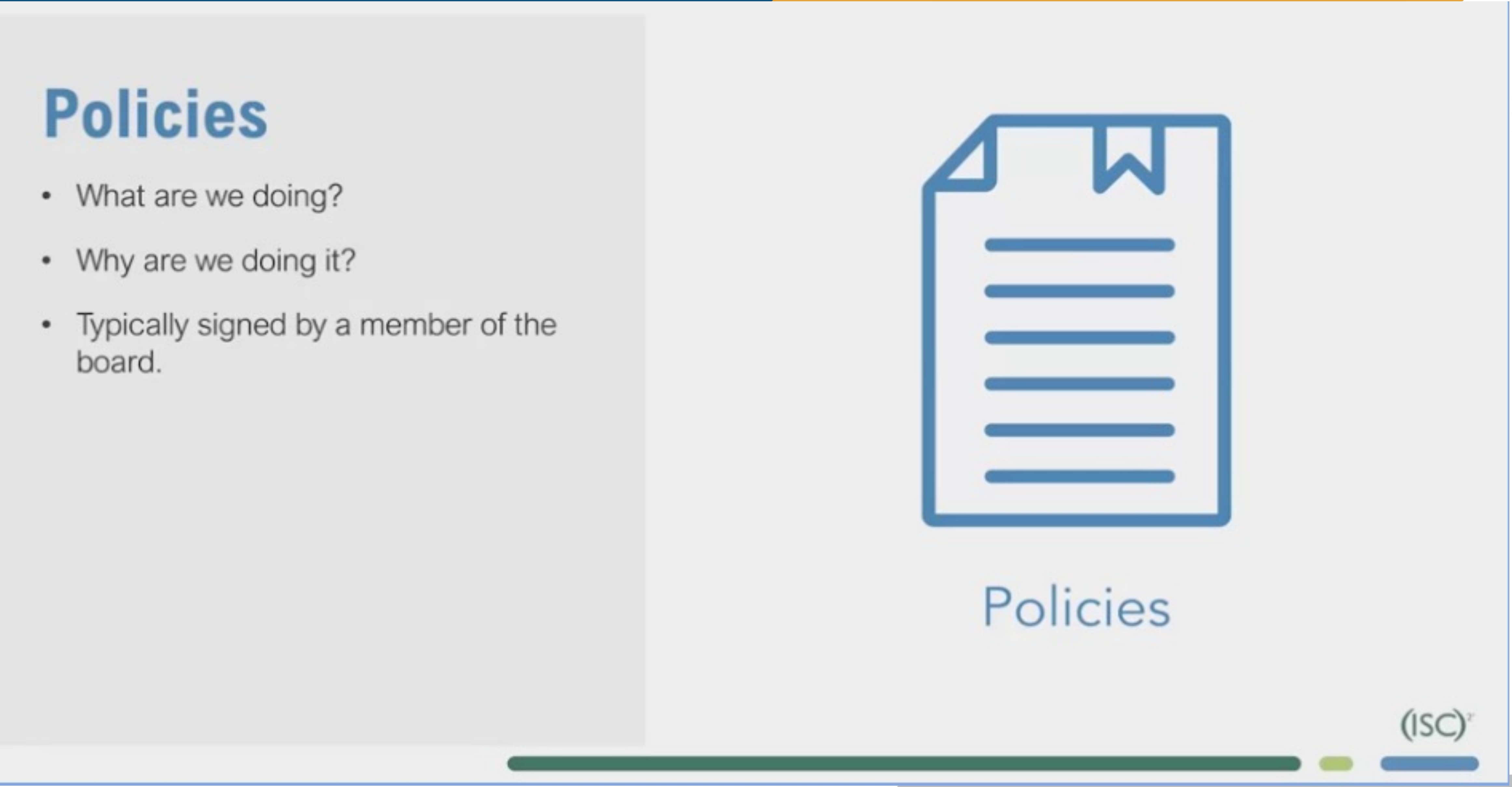
Regulations

(ISC)²



Standards

- ISO27001
- ISO27032
- NIST SP800-53
- NIST Cyber Security Framework

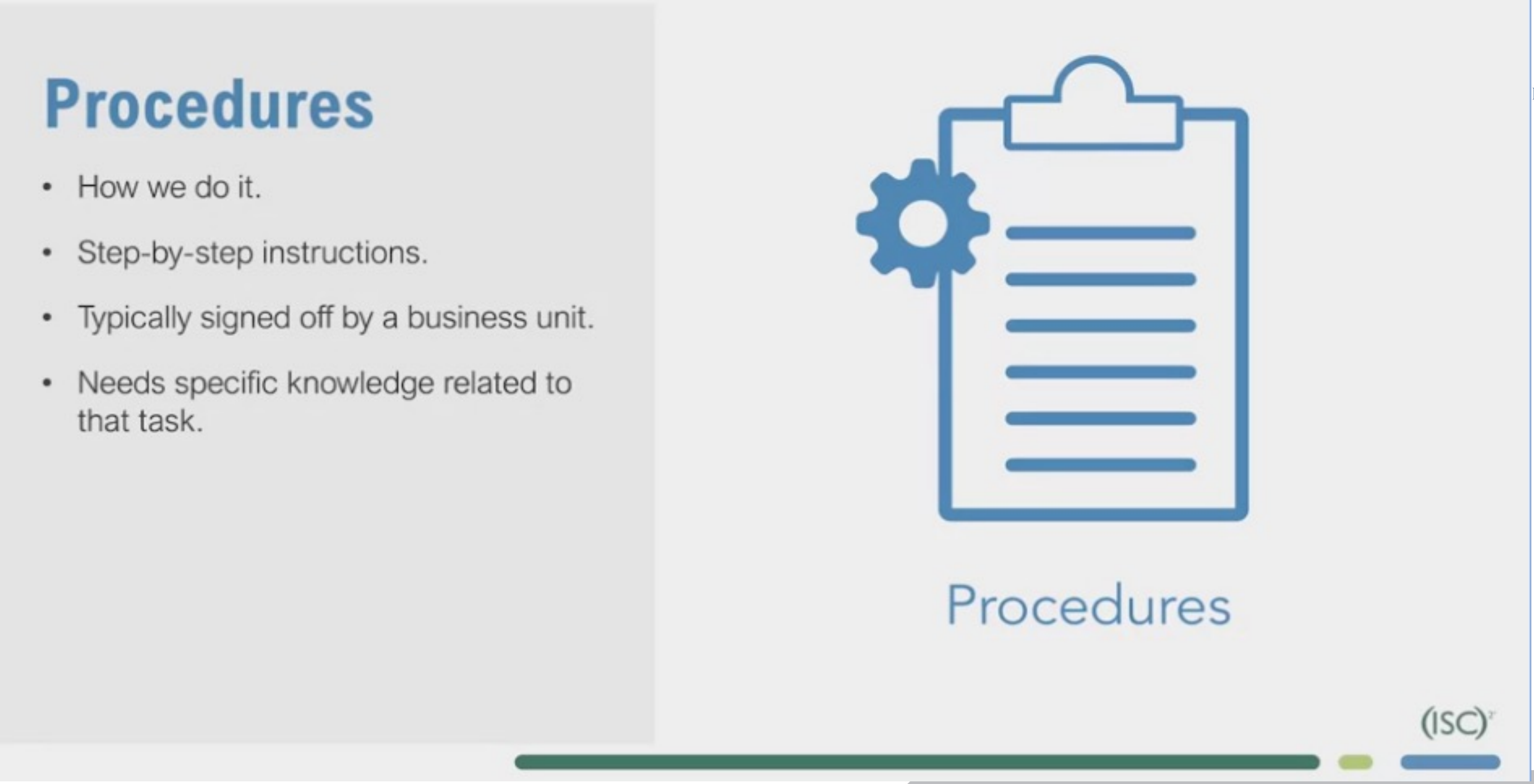


Policies

- What are we doing?
- Why are we doing it?
- Typically signed by a member of the board.

Policies

(ISC)^2



Procedures

- How we do it.
- Step-by-step instructions.
- Typically signed off by a business unit.
- Needs specific knowledge related to that task.

Governance Elements

- Any business or organization exists to fulfill a purpose, whether it is to provide raw materials to an industry, manufacture equipment to build computer hardware, develop software applications, construct buildings or provide goods and services
- To complete the objective requires that decisions are made, rules and practices are defined, and policies and procedures are in place to guide the organization in its pursuit of achieving its goals and mission
- When leaders and management implement the systems and structures that the organization will use to achieve its goals, they are guided by laws and regulations created by governments to enact public policy. Laws and regulations guide the development of standards, which cultivate policies, which result in procedures

Governance Elements

How are regulations, standards, policies and procedures related? It might help to look at the list in reverse

- Procedures are the detailed steps to complete a task that support departmental or organizational policies
- Policies are put in place by organizational governance, such as executive management, to provide guidance in all activities to ensure that the organization supports industry standards and regulations
- Standards are often used by governance teams to provide a framework to introduce policies and procedures in support of regulations
- Regulations are commonly issued in the form of laws, usually from government (not to be confused with governance) and typically carry financial penalties for noncompliance

Governance Elements: Regulations and Laws

- Regulations and associated fines and penalties can be imposed by governments at the national, regional or local level
- Because regulations and laws can be imposed and enforced differently in different parts of the world, here are a few examples to connect the concepts to actual regulations
- The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is an example of a law that governs the use of protected health information (PHI) in the United States
- Violation of the HIPAA rule carries the possibility of fines and/or imprisonment for both individuals and companies.

Governance Elements: Regulations and Laws

- The General Data Protection Regulation (GDPR) was enacted by the European Union (EU) to control use of Personally Identifiable Information (PII) of its citizens and those in the EU
- It includes provisions that apply financial penalties to companies who handle data of EU citizens and those living in the EU even if the company does not have a physical presence in the EU, giving this regulation an international reach
- Finally, it is common to be subject to regulation on several levels. Multinational organizations are subject to regulations in more than one nation in addition to multiple regions and municipalities
- Organizations need to consider the regulations that apply to their business at all levels—national, regional and local—and ensure they are compliant with the most restrictive regulation

Governance Elements: Standards

- Organizations use multiple standards as part of their information systems security programs, both as compliance documents and as advisories or guidelines
- Standards cover a broad range of issues and ideas and may provide assurance that an organization is operating with policies and procedures that support regulations and are widely accepted best practices
- The International Organization for Standardization (ISO) develops and publishes international standards on a variety of technical subjects, including information systems and information security, as well as encryption standards
- ISO solicits input from the international community of experts to provide input on its standards prior to publishing. Documents outlining ISO standards may be purchased online

Governance Elements: Standards

- The National Institute of Standards and Technology (NIST) is a United States government agency under the Department of Commerce and publishes a variety of technical standards in addition to information technology and information security standards
- Many of the standards issued by NIST are requirements for U.S. government agencies and are considered recommended standards by industries worldwide. NIST standards solicit and integrate input from industry and are free to download from the NIST website
- Finally, think about how computers talk to other computers across the globe. People speak different languages and do not always understand each other

Governance Elements: Policies

- Policy is informed by applicable law(s) and specifies which standards and guidelines the organization will follow
- Policy is broad, but not detailed; it establishes context and sets out strategic direction and priorities
- Governance policies are used to moderate and control decision-making, to ensure compliance when necessary and to guide the creation and implementation of other policies
- Policies are often written at many levels across the organization
- High-level governance policies are used by senior executives to shape and control decision-making processes

Governance Elements: Policies

- Other high-level policies direct the behaviour and activity of the entire organization as it moves toward specific or general goals and objectives
- Functional areas such as human resources management, finance and accounting, and security and asset protection usually have their own sets of policies
- Whether imposed by laws and regulations or by contracts, the need for compliance might also require the development of specific high-level policies that are documented and assessed for their effective use by the organization.

Governance Elements: Procedures

- Procedures define the explicit, repeatable activities necessary to accomplish a specific task or set of tasks
- They provide supporting data, decision criteria or other explicit knowledge needed to perform each task. Procedures can address one-time or infrequent actions or common, regular occurrences
- In addition, procedures establish the measurement criteria and methods to use to determine whether a task has been successfully completed
- Properly documenting procedures and training personnel on how to locate and follow them is necessary for deriving the maximum organizational benefits from procedures

(ISC)2 Code of Ethics

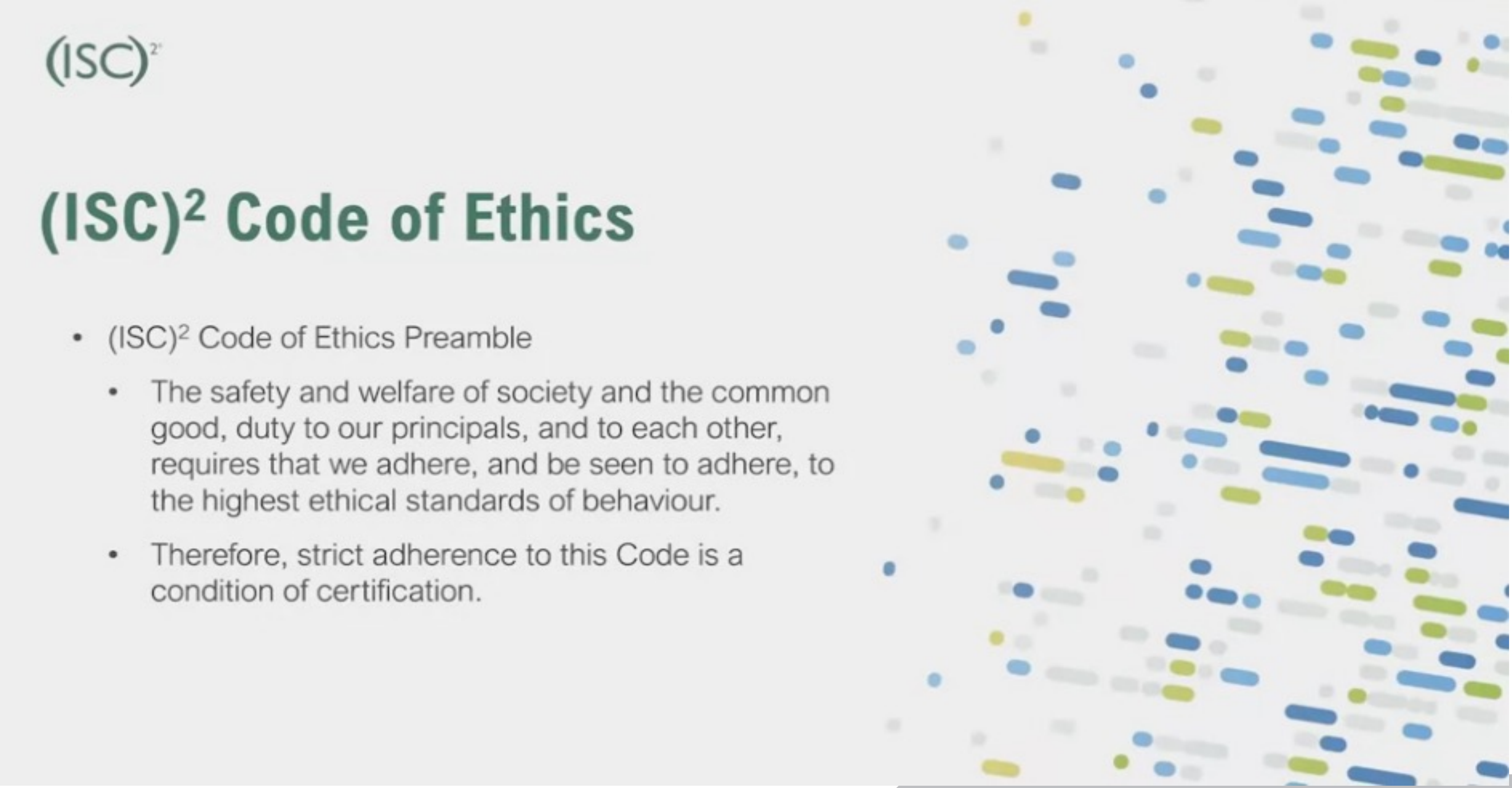
(ISC)²

Module Overview

- What are Ethics?
- (ISC)² Code of Ethics

What are Ethics?

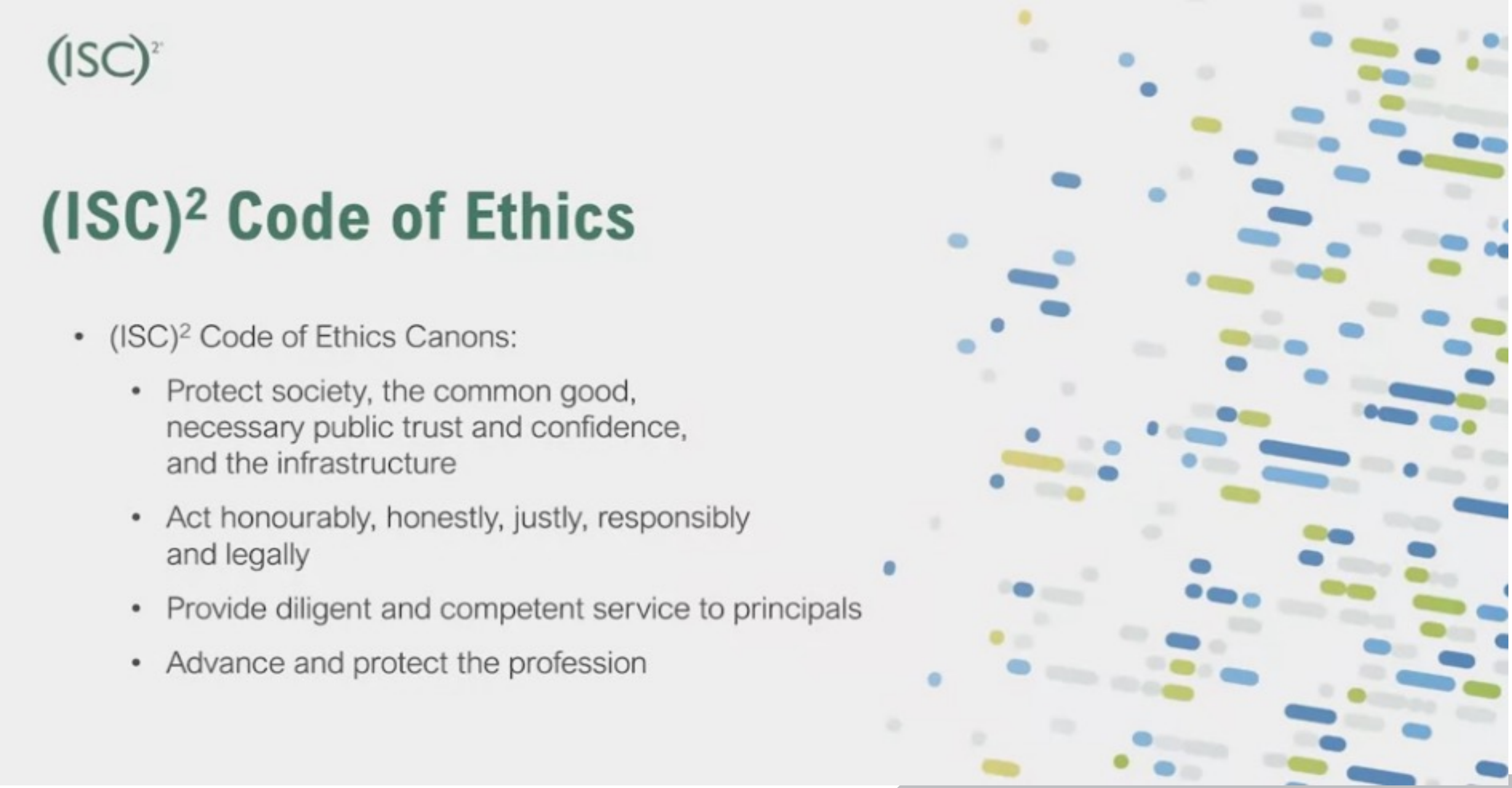
- Society, culture and law
- Globalization
- What is ethical?



(ISC)²

(ISC)² Code of Ethics

- (ISC)² Code of Ethics Preamble
  - The safety and welfare of society and the common good, duty to our principals, and to each other, requires that we adhere, and be seen to adhere, to the highest ethical standards of behaviour.
  - Therefore, strict adherence to this Code is a condition of certification.



(ISC)²

(ISC)² Code of Ethics

- (ISC)² Code of Ethics Canons:
  - Protect society, the common good, necessary public trust and confidence, and the infrastructure
  - Act honourably, honestly, justly, responsibly and legally
  - Provide diligent and competent service to principals
  - Advance and protect the profession

Professional Code of Conduct

- All information security professionals who are certified by (ISC)^2 recognize that certification is a privilege that must be both earned and maintained. Every (ISC)^2 member is required to commit to fully support the Canons of the (ISC)^2 Code of Ethics. For more information on the Code of Ethics, please visit https://www.isc2.org/Ethics
- The preamble states the purpose and intent of the (ISC)^2 Code of Ethics
- The Canons represent the important beliefs held in common by the members of (ISC)^2. The most important tenets are listed first, followed by the rest in order of priority

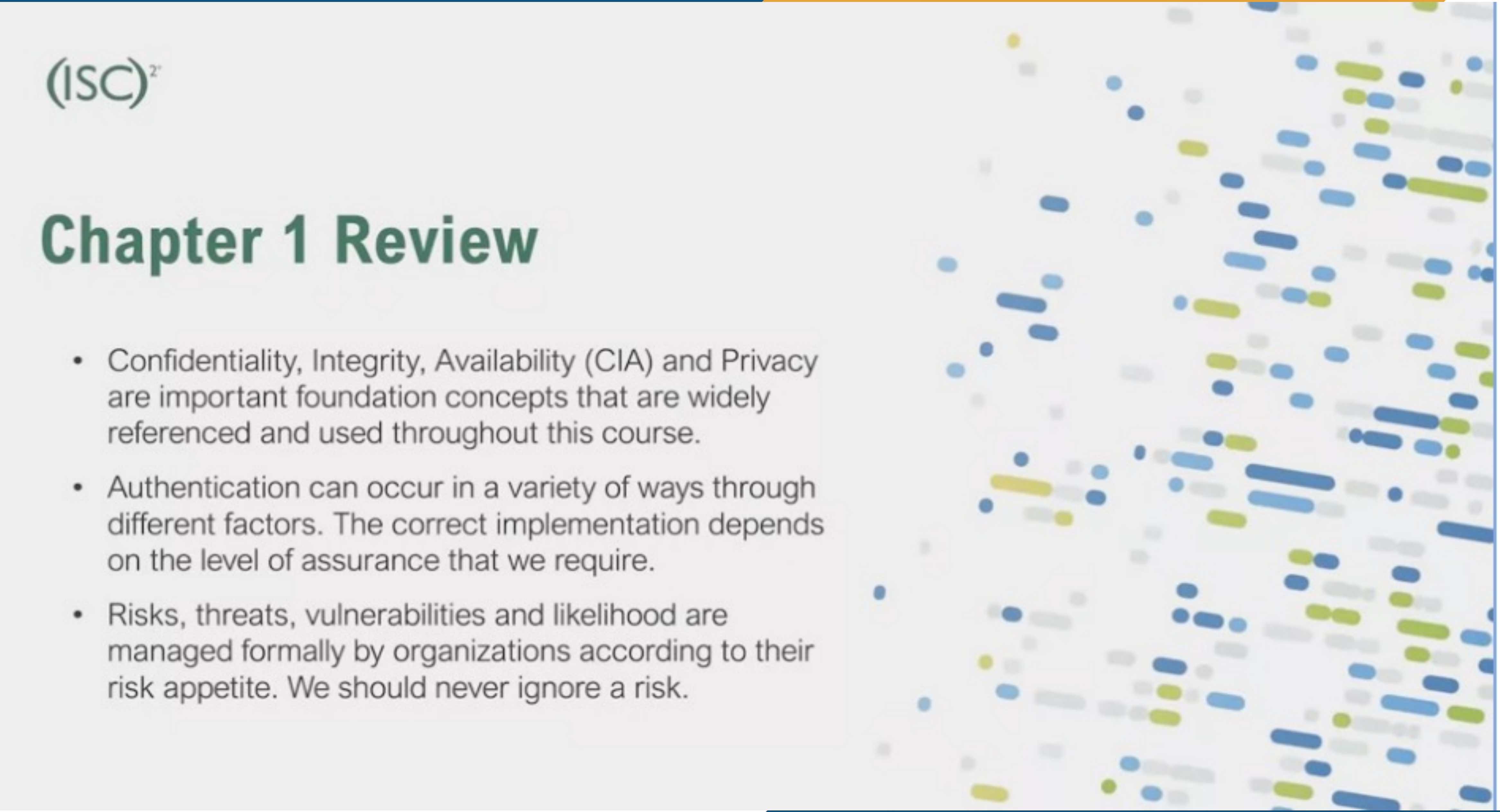
(ISC)^2 Code of Ethics Preamble

- The safety and welfare of society and the common good, duty to our principals, and to each other, requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior

(ISC)^2 Code of Ethics Canons

The (ISC)^2 member is expected to do the following:

- Protect society, the common good, necessary public trust and confidence, and the infrastructure
- Act honourably, honestly, justly, responsibly, and legally
- Provide diligent and competent service to principals
- Advance and protect the profession



(ISC)²

Chapter 1 Review

- Confidentiality, Integrity, Availability (CIA) and Privacy are important foundation concepts that are widely referenced and used throughout this course.
- Authentication can occur in a variety of ways through different factors. The correct implementation depends on the level of assurance that we require.
- Risks, threats, vulnerabilities and likelihood are managed formally by organizations according to their risk appetite. We should never ignore a risk.

Course Summary

- In this course, we covered security principles, starting with concepts of information assurance
- We highlighted the CIA triad as the primary components of information assurance
- The “C” stands for confidentiality; we must protect the data that needs protection and prevent access to unauthorized individuals
- The “I” represents integrity; we must ensure the data has not been altered in an unauthorized manner
- The “A” symbolizes availability; we must make sure data is accessible to authorized users when and where it is needed, and in the form and format that is required. We also discussed the importance of privacy, authentication, non-repudiation and authorization.

Course Summary

- We explored the safeguards and countermeasures prescribed for an information system to protect the confidentiality, integrity and availability of the system and its information
- By applying risk management, we were able to assess and prioritize the risks (asset vulnerabilities that can be exploited by threats) to an organization
- An organization can decide whether to accept the risk (ignoring the risks and continuing risky activities), avoid the risk (ceasing the risky activity to remove the likelihood that an event will occur), mitigate the risk (taking action to prevent or reduce the impact of an event), or transfer the risk (passing risk to a third party).

Course Summary

- We then learned about three types of security controls: physical, technical and administrative
- They act as safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity and availability of the system and its information
- The implementation of security controls should reduce risk, hopefully to an acceptable level
- Physical controls address process-based security needs using physical hardware devices, such as a badge reader, architectural features of buildings and facilities, and specific security actions taken by people
- Technical controls (also called logical controls) are security controls that computer systems and networks directly implement. Administrative controls (also known as managerial controls) are directives, guidelines or advisories aimed at the people within the organization

Course Summary

- We were then introduced to organizational security roles and governance, the policies and procedures that shape organizational management and drive decision-making
- As discussed, we typically derive procedures from policies, policies from standards, standards from regulations
- Regulations are commonly issued in the form of laws, usually from government (not to be confused with governance) and typically carry financial penalties for noncompliance. Standards are often used by governance teams to provide a framework to introduce policies and procedures in support of regulations
- Policies are put in place by organizational governance, such as executive management, to provide guidance in all activities to ensure the organization supports industry standards and regulations
- Procedures are the detailed steps to complete a task that will support departmental or organizational policies.
- Finally, we covered the (ISC)^2 Code of Ethics, which members of the organization commit to fully support. Bottom line, we must act legally and ethically in the field of cybersecurity

Terms and Definitions

- **Adequate Security** - Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse or unauthorized access to or modification of information. Source: OMB Circular A-130
- **Administrative Controls** - Controls implemented through policy and procedures. Examples include access control processes and requiring multiple personnel to conduct a specific operation. Administrative controls in modern environments are often enforced in conjunction with physical and/or technical controls, such as an access-granting policy for new users that requires login and approval by the hiring manager
- **Artificial Intelligence** - The ability of computers and robots to simulate human intelligence and behaviour

Terms and Definitions

- **Asset** - Anything of value that is owned by an organization. Assets include both tangible items such as information systems and physical property and intangible assets such as intellectual property
- **Authentication** - Access control process validating that the identity being claimed by a user or entity is known to the system, by comparing one (single factor or SFA) or more (multi-factor authentication or MFA) factors of identification
- **Authorization** - The right or a permission that is granted to a system entity to access a system resource. NIST 800-82 Rev.2

Terms and Definitions

- **Availability** - Ensuring timely and reliable access to and use of information by authorized users
- **Baseline** - A documented, lowest level of security configuration allowed by a standard or organization
- **Bot** - Malicious code that acts like a remotely controlled “robot” for an attacker, with other Trojan and worm capabilities
- **Classified or Sensitive Information** - Information that has been determined to require protection against unauthorized disclosure and is marked to indicate its classified status and classification level when in documentary form

Terms and Definitions

- **Confidentiality** - The characteristic of data or information when it is not made available or disclosed to unauthorized persons or processes. NIST 800-66
- **Criticality** - A measure of the degree to which an organization depends on the information or information system for the success of a mission or of a business function. NIST SP 800-60 Vol. 1, Rev. 1
- **Data Integrity** - The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing and while in transit. Source: NIST SP 800-27 Rev A

Terms and Definitions

- **Encryption** - The process and act of converting the message from its plaintext to ciphertext. Sometimes it is also referred to as enciphering. The two terms are sometimes used interchangeably in literature and have similar meanings.
- **General Data Protection Regulation (GDPR)** - In 2016, the European Union passed comprehensive legislation that addresses personal privacy, deeming it an individual human right.
- **Governance** -The process of how an organization is managed; usually includes all aspects of how decisions are made for that organization, such as policies, roles, and procedures the organization uses to make those decisions.

Terms and Definitions

- **Health Insurance Portability and Accountability Act (HIPAA)** - This U.S. federal law is the most important healthcare information regulation in the United States. It directs the adoption of national standards for electronic healthcare transactions while protecting the privacy of individual's health information. Other provisions address fraud reduction, protections for individuals with health insurance and a wide range of other healthcare-related activities. Est. 1996.
- **Impact** - The magnitude of harm that could be caused by a threat's exercise of a vulnerability.
- **Information Security Risk** - The potential adverse impacts to an organization's operations (including its mission, functions and image and reputation), assets, individuals, other organizations, and even the nation, which results from the possibility of unauthorized access, use, disclosure, disruption, modification or destruction of information and/or information systems.

Terms and Definitions

- **Institute of Electrical and Electronics Engineers** - IEEE is a professional organization that sets standards for telecommunications, computer engineering and similar disciplines
- **Integrity** - The property of information whereby it is recorded, used and maintained in a way that ensures its completeness, accuracy, internal consistency and usefulness for a stated purpose
- **International Organization of Standards (ISO)** - The ISO develops voluntary international standards in collaboration with its partners in international standardization, the International Electro-technical Commission (IEC) and the International Telecommunication Union (ITU), particularly in the field of information and communication technologies

Terms and Definitions

- **Internet Engineering Task Force (IETF)** - The internet standards organization, made up of network designers, operators, vendors and researchers, that defines protocol standards (e.g., IP, TCP, DNS) through a process of collaboration and consensus. Source: NIST SP 1800-16B
- **Likelihood** - The probability that a potential vulnerability may be exercised within the construct of the associated threat environment
- **Likelihood of Occurrence** - A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or set of vulnerabilities
- **Multi-Factor Authentication** - Using two or more distinct instances of the three factors of authentication (something you know, something you have, something you are) for identity verification.

Terms and Definitions

- **National Institutes of Standards and Technology (NIST)** - The NIST is part of the U.S. Department of Commerce and addresses the measurement infrastructure within science and technology efforts within the U.S. federal government. NIST sets standards in a number of areas, including information security within the Computer Security Resource Center of the Computer Security Divisions
- **Non-repudiation** - The inability to deny taking an action such as creating information, approving information and sending or receiving a message
- **Personally Identifiable Information (PII) -** The National Institute of Standards and Technology, known as NIST, in its Special Publication 800-122 defines PII as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial and employment information."

Terms and Definitions

- **Physical Controls** - Controls implemented through a tangible mechanism. Examples include walls, fences, guards, locks, etc. In modern organizations, many physical control systems are linked to technical/logical systems, such as badge readers connected to door locks.
- **Privacy** - The right of an individual to control the distribution of information about themselves.
- **Probability -** The chances, or likelihood, that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities. Source: NIST SP 800-30 Rev.
- **Protected Health Information (PHI)** - Information regarding health status, the provision of healthcare or payment for healthcare as defined in HIPAA (Health Insurance Portability and Accountability Act).

Terms and Definitions

- **Qualitative Risk Analysis** - A method for risk analysis that is based on the assignment of a descriptor such as low, medium or high. Source: NISTIR 8286
- **Quantitative Risk Analysis** - A method for risk analysis where numerical values are assigned to both impact and likelihood based on statistical probabilities and monetarized valuation of loss or gain. Source: NISTIR 8286
- **Risk** - A possible event which can have a negative impact upon the organization.
- **Risk Acceptance** - Determining that the potential benefits of a business function outweigh the possible risk impact/likelihood and performing that business function with no other action.
- **Risk Assessment** - The process of identifying and analyzing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals and other organizations. The analysis performed as part of risk management which incorporates threat and vulnerability analyses and considers mitigations provided by security controls planned or in place.

Terms and Definitions

- **Risk Avoidance** - Determining that the impact and/or likelihood of a specific risk is too great to be offset by the potential benefits and not performing a certain business function because of that determination.
- **Risk Management** - The process of identifying, evaluating and controlling threats, including all the phases of risk context (or frame), risk assessment, risk treatment and risk monitoring.
- **Risk Management Framework** - A structured approach used to oversee and manage risk for an enterprise. Source: CNSSI 4009
- **Risk Mitigation** - Putting security controls in place to reduce the possible impact and/or likelihood of a specific risk.
- **Risk Tolerance** - The level of risk an entity is willing to assume in order to achieve a potential desired result. Source: NIST SP 800-32. Risk threshold, risk appetite and acceptable risk are also terms used synonymously with risk tolerance.

Terms and Definitions

- **Risk Transference** - Paying an external party to accept the financial impact of a given risk.
- **Risk Treatment** - The determination of the best way to address an identified risk.
- **Security Controls** - The management, operational and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity and availability of the system and its information. Source: FIPS PUB 199
- **Sensitivity** - A measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection. Source: NIST SP 800-60 Vol 1 Rev 1
- **Single-Factor Authentication** - Use of just one of the three available factors (something you know, something you have, something you are) to carry out the authentication process being requested.
- **State** - The condition an entity is in at a point in time.

Terms and Definitions

- **System Integrity** - The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental. Source: NIST SP 800-27 Rev. A
- **Technical Controls** - Security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software or firmware components of the system.
- **Threat** - Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image or reputation), organizational assets, individuals, other organizations or the nation through an information system via unauthorized access, destruction, disclosure, modification of information and/or denial of service.

Terms and Definitions

- **Threat Actor** - An individual or a group that attempts to exploit vulnerabilities to cause or force a threat to occur
- **Threat Vector** - The means by which a threat actor carries out their objectives
- **Token** - A physical object a user possesses and controls that is used to authenticate the user’s identity. Source: NISTIR 7711
- **Vulnerability** - Weakness in an information system, system security procedures, internal controls or implementation that could be exploited by a threat source. Source: NIST SP 800-30 Rev 1