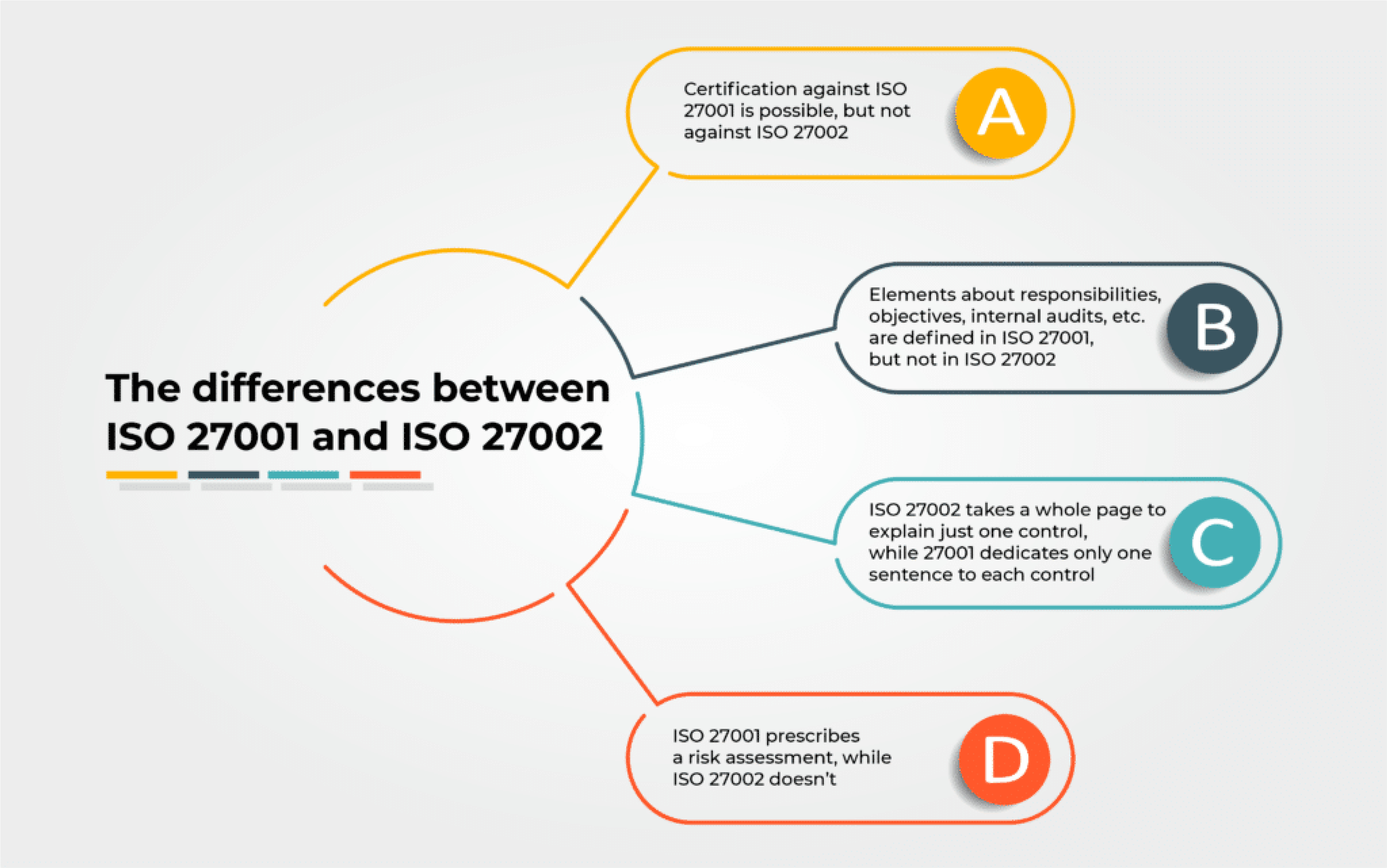
ISO 27001

ISO/IEC 27001:2022 is a standard for **information security management systems (ISMS)** that provides guidance for establishing, implementing, maintaining, and continually improving an information security management system [1]. It is the world's best-known standard for ISMS and is applicable to companies of any size and from all sectors of activity [1]. The standard defines requirements that an ISMS must meet and provides a tool for risk management, cyber-resilience, and operational excellence [1].
The standard was most recently established in 2022 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) [1]. It replaces the previous version, ISO/IEC 27001:2013, and includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization [2].



The differences between ISO 27001 and ISO 27002

A Certification against ISO 27001 is possible, but not against ISO 27002

B Elements about responsibilities, objectives, internal audits, etc. are defined in ISO 27001, but not in ISO 27002

C ISO 27002 takes a whole page to explain just one control, while 27001 dedicates only one sentence to each control

D ISO 27001 prescribes a risk assessment, while ISO 27002 doesn't