WWW.VSE.CZ

Seventeen Years With the ISO/IEC 27k Family of Standards

PETR DOUCEK, LEA NEDOMOVÁ, MILOS MARYSKA

Prague University of Economics and Business

doucek@vse.cz; nedomova@vse.cz; milos.maryska @vse.cz

Agenda

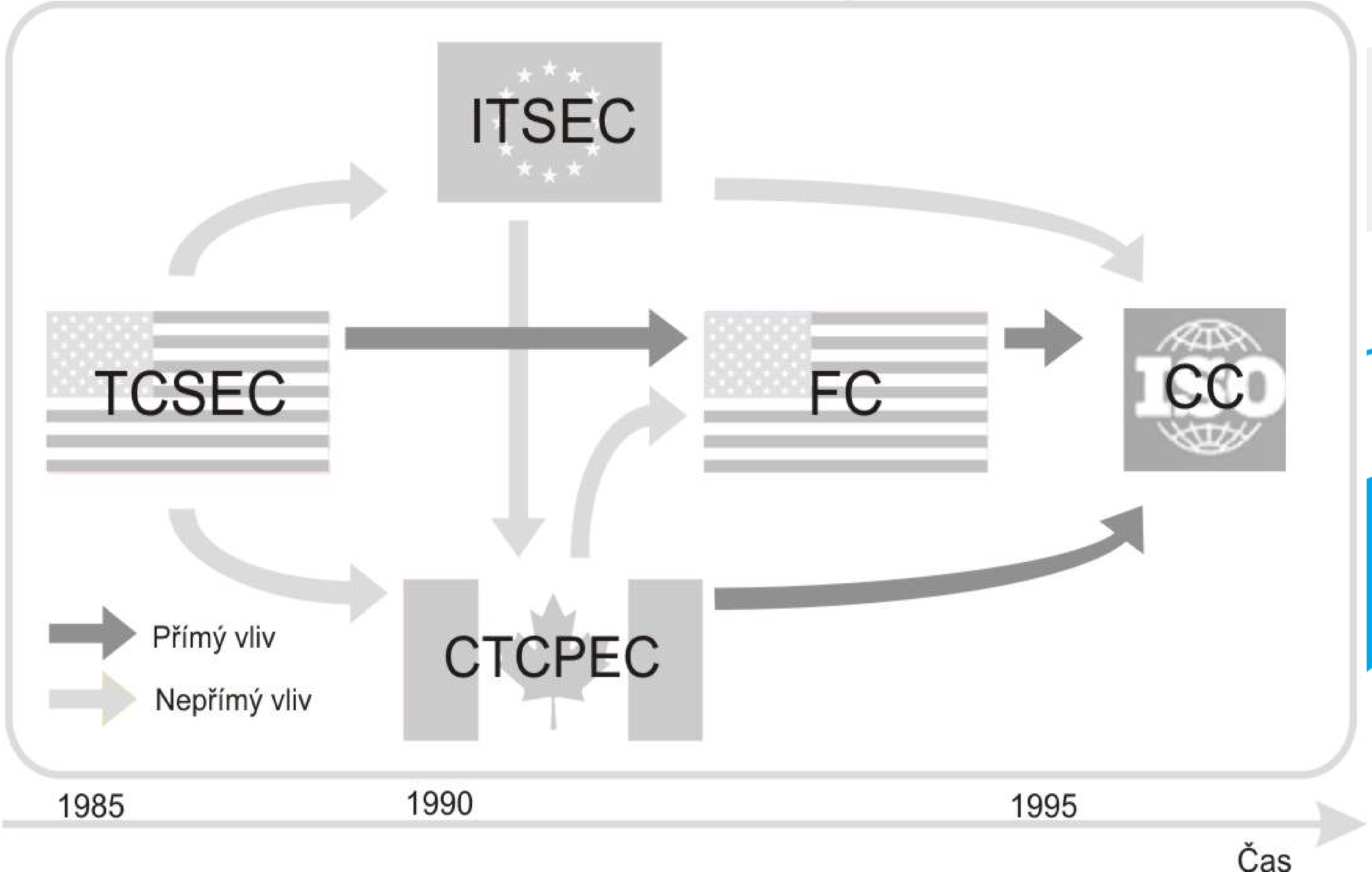
- ISO/IEC 27000 From dark history to the present
- Structure of the norm ISO/IEC 27002:2022.
  - Comparison to the old one
- Expected changes in 27k family
- Conclusions

Introduction

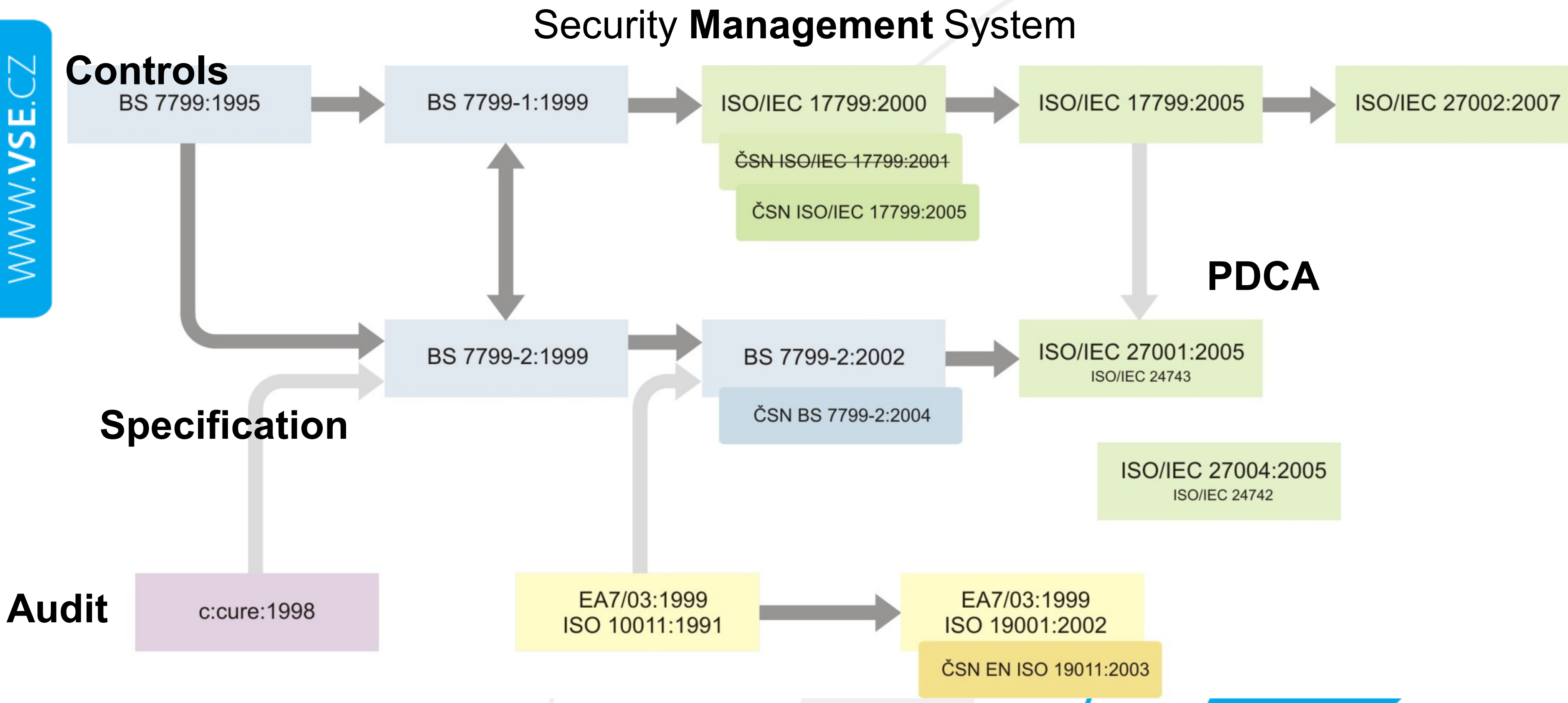
The current penetration of information systems into the economy, including its current globalization, practically makes all our activities critically dependent on information systems. Dependence on digital data also requires to trust them. Users' trust in the data in information systems is one of the fundamental features of the security of information systems. Cyberspace action associated with the war in Ukraine clearly show the importance of protecting data. Since there are no borders in cyberspace, any attack between the parties to the conflict has an impact on their surroundings, allies and sympathizers. There is a reason why the National Cyber and Information Security Agency issues a warning about cyber-attacks against authorities and organizations in the Czech Republic.

ISO/IEC 27000 From the Dark History to the Present

Security **Evaluation** Criteria



ISO/IEC 27000 From the Dark History to the Present



Security **Management** System

Controls

BS 7799:1995

BS 7799-1:1999

ISO/IEC 17799:2000

~~ČSN ISO/IEC 17799:2001~~

ČSN ISO/IEC 17799:2005

ISO/IEC 17799:2005

ISO/IEC 27002:2007

PDCA

BS 7799-2:1999

BS 7799-2:2002

ČSN BS 7799-2:2004

ISO/IEC 27001:2005
ISO/IEC 24743

ISO/IEC 27004:2005
ISO/IEC 24742

Specification

Audit

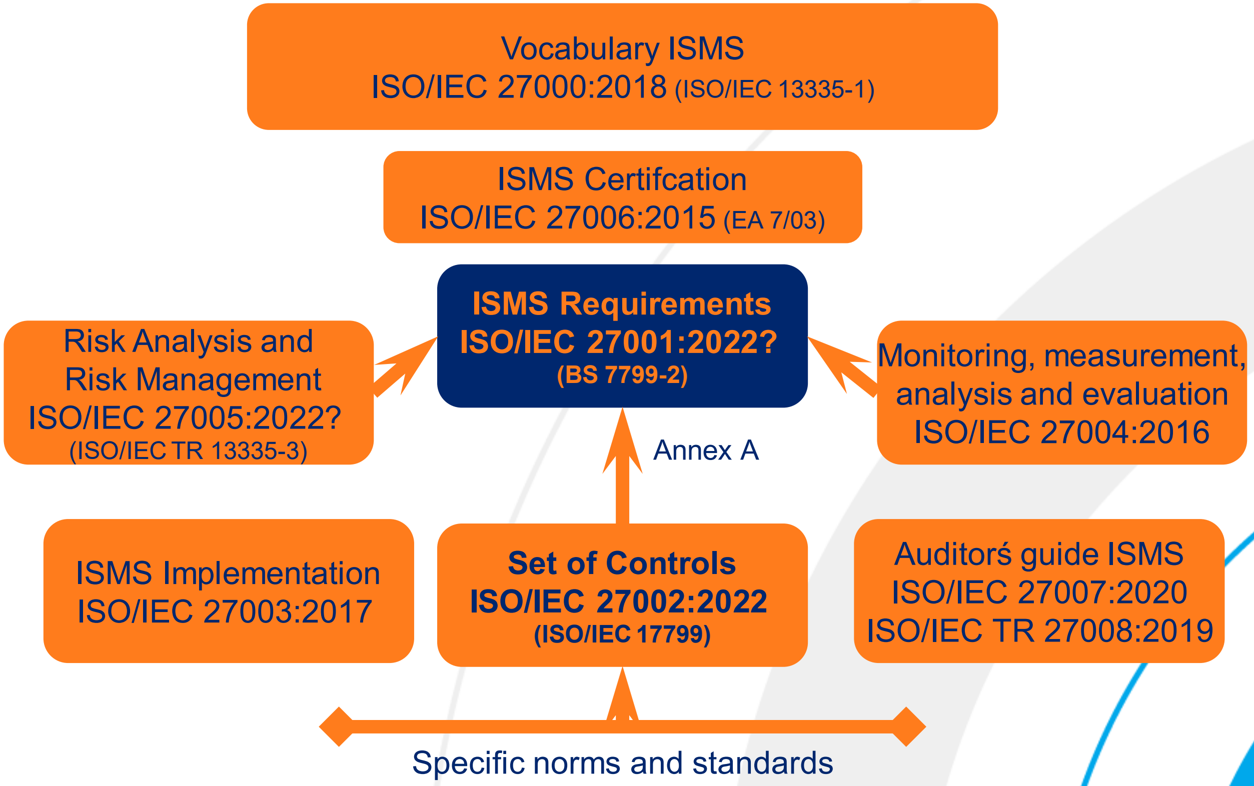
c:cure:1998

EA7/03:1999
ISO 10011:1991

EA7/03:1999
ISO 19001:2002

ČSN EN ISO 19011:2003

ISO/IEC 27000 From the Dark History to the Present



Vocabulary ISMS
ISO/IEC 27000:2018 (ISO/IEC 13335-1)

ISMS Certifcation
ISO/IEC 27006:2015 (EA 7/03)

Risk Analysis and
Risk Management
ISO/IEC 27005:2022?
(ISO/IEC TR 13335-3)

ISMS Requirements
ISO/IEC 27001:2022?
(BS 7799-2)

Monitoring, measurement,
analysis and evaluation
ISO/IEC 27004:2016

Annex A

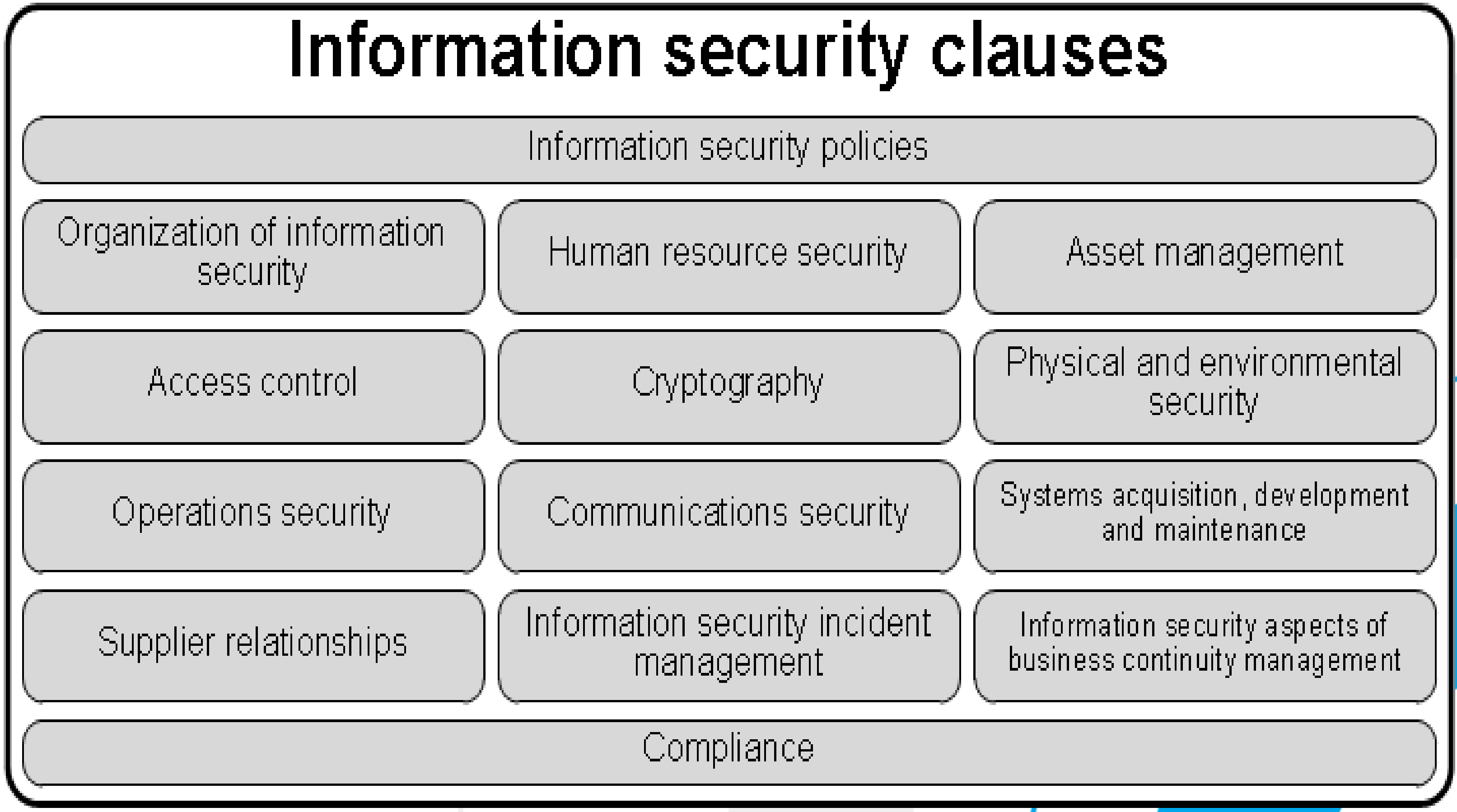
ISMS Implementation
ISO/IEC 27003:2017

Set of Controls
ISO/IEC 27002:2022
(ISO/IEC 17799)

Auditorś guide ISMS
ISO/IEC 27007:2020
ISO/IEC TR 27008:2019

Specific norms and standards

ISO/IEC 27001:2013 - Structure



Information security clauses

Information security policies

Organization of information security

Human resource security

Asset management

Access control

Cryptography

Physical and environmental security

Operations security

Communications security

Systems acquisition, development and maintenance

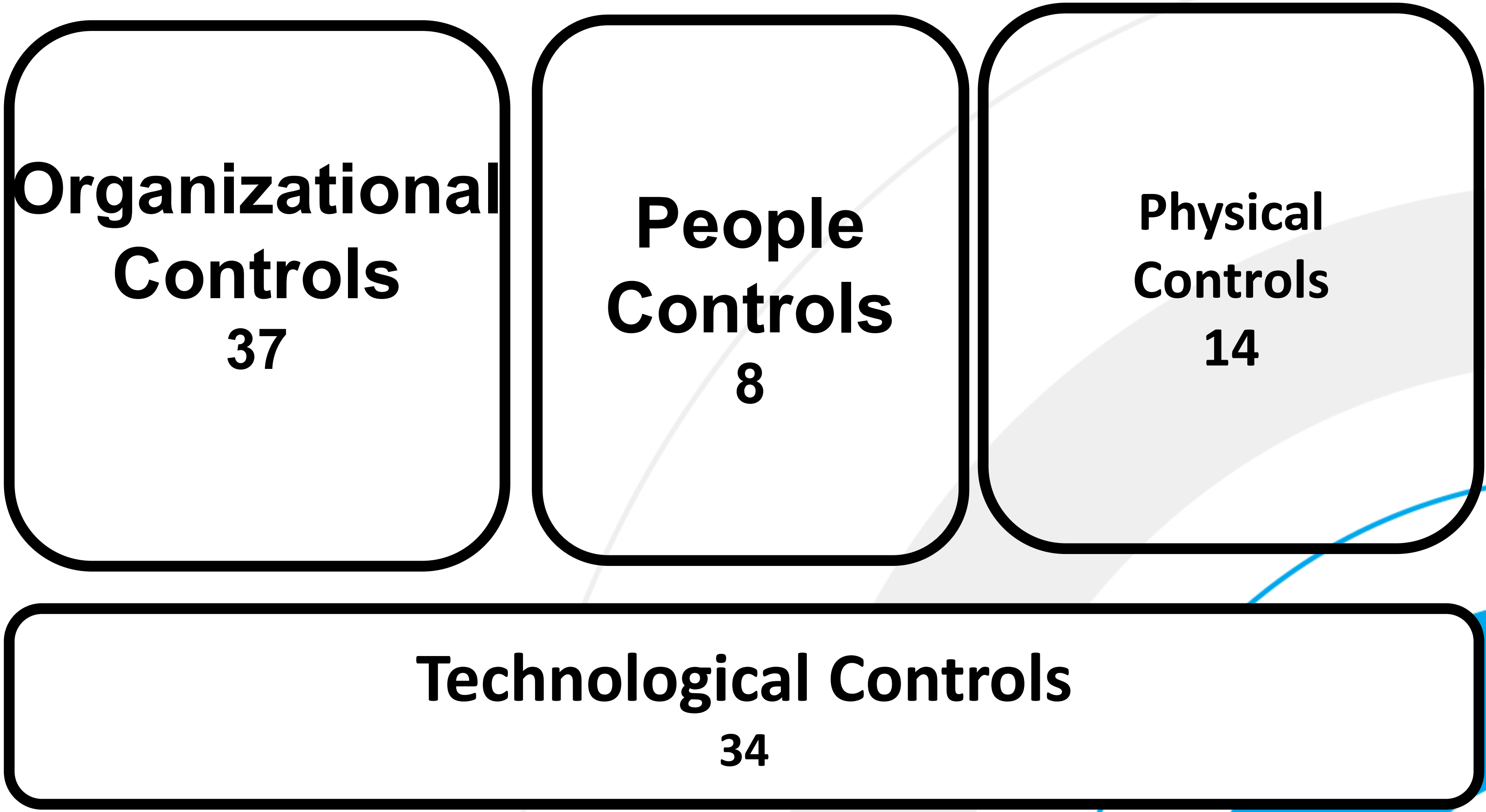
Supplier relationships

Information security incident management

Information security aspects of business continuity management

Compliance

ISO/IEC 27002:2022 - Structure



Organizational Controls
37

People Controls
8

Physical Controls
14

Technological Controls
34

It evokes requirements for ISO/IEC 27001 changes

WWW.VSE.CZ

The layout of the standard has also improved in terms of individual controls. The layout for each control contains the following:

Control title: Short name of the control;

Attribute table: A table shows the value(s) of each attribute for the given control;

Example for control “Policies for Information Security”

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality#Integrity#Availability	#Identify	#Governance	#Governance_and_Eco-system #Resilience

Conclusions

- An effective tool for managing information security at the business organization level
- Permanent maintenend system
- Relatively short reaction time on new trendy in security.
- Best practices.
- New standards – cyber security ISO/IEC 27100
- Impacts on local legal frame.

Questions by e-mail?

Seventeen Years With the ISO/IEC 27k Family of Standards

PETR DOUCEK, LEA NEDOMOVÁ, MILOS MARYSKA

PRAGUE UNIVERSITY OF ECONOMICS AND BUSINESS

WWW.VSE.CZ