ISO 27001 Framework for Securing Election Infrastructure and Machine Voting

2022 International Conference on Information Technologies (InfoTech-2022), Proceedings of the IEEE Conference, Rec # 55606

15-16 September 2022, Bulgaria

Veselin Monev, PhD

ISO 27001 Framework for Securing Election Infrastructure and Machine Voting

Problem

- E-voting (machine voting) infrastructure needs to be secured with best practices from the information security theory;
- Use case: Government entities tasked with protecting the integrity of the political vote;
- Limited research on a holistic set of security policies and controls that focuses on securing e-voting infrastructure;
- Limited guidelines for complying with security frameworks, such as ISO 27001.

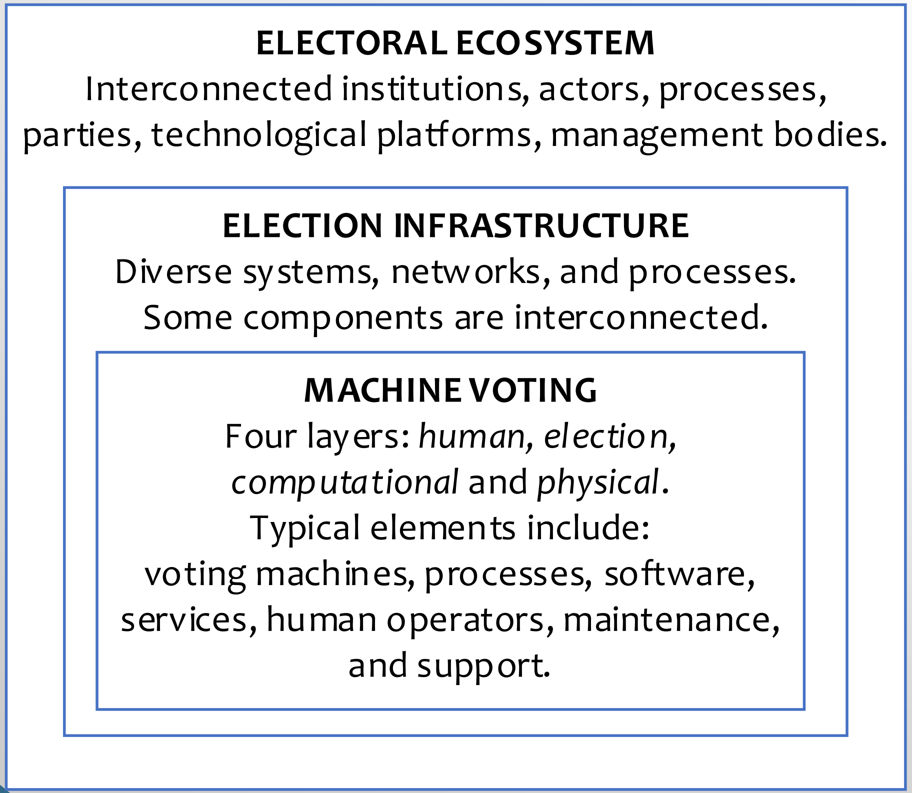
Solution

- An Information Security Framework tailored to the specifics of machine voting infrastructure and government processes.
- Guidelines for complying with a specific information security framework, such as the ISO 27001 standard.

ISO 27001 Framework for Securing Election Infrastructure and Machine Voting

Election Infrastructure

- Need to identify the specific assets and functions.



ELECTORAL ECOSYSTEM
Interconnected institutions, actors, processes, parties, technological platforms, management bodies.

ELECTION INFRASTRUCTURE
Diverse systems, networks, and processes. Some components are interconnected.

MACHINE VOTING
Four layers: *human, election, computational* and *physical*.
Typical elements include:
voting machines, processes, software, services, human operators, maintenance, and support.

Information security goals

- Confidentiality, integrity, availability;
- Reliability of systems;
- Anonymity of voters;
- Accountability of systems;
- Auditability / disclosability of software and hardware;
- Usability of interfaces;
- Documentation;
- Moral integrity of personnel;
- Compliance.

ISO 27001 Framework for Securing Election Infrastructure and Machine Voting

Considerations:

- Implementation approaches vary among political organisations due to differences in the electoral ecosystem and used technology;
- The most crucial goal is the protection of the integrity of the vote;
- The adoption of a single security standard, such as ISO 27001, may be insufficient;
- All components of the election infrastructure should be protected;
- The scope of ISO 27001 should include all organisations that are responsible for the protection;
- The public is a specific interested party;
- Legal frameworks and hence requirements vary;
- Responsible government agency for the security policy needs to be established;
- Meticulous vulnerability management process;
- Risks related to the election infrastructure assets should be kept low;
- Advanced security awareness and training programme;
- Trained professionals need to monitor and maintain the infrastructure;

ISO 27001 Framework for Securing Election Infrastructure and Machine Voting

- Documented key processes are essential;
- Performance measurement should be tailored to the security goals;
- Audit and assessment teams should be familiar with the security of e-voting infrastructure;
- Above a certain level of risk, e-voting should not be allowed;
- Non-mandatory security policies should be drafted to support controls;
- Adopting the zero-trust concept to protect networks;
- Advanced security monitoring during the entire lifecycle of voting machines;
- Permanent isolation of voting machines from insecure networks (the Internet);
- Sophisticated third party risk management process;
- Need for a business continuity management programme;
- Recommended high degree of process automation.