CISQ Standards for Federal Systems

Dr. Bill Curtis
Founding Executive Director, CISQ
Washington, DC
May 1, 2019
Why Do Software-Intensive System Projects Fail?

Failure causes
- Unrealistic expectations
- Incomplete requirements
- Weak contracts & control
- Unachievable schedules, budgets
- Changing requirements
- Unsound architecture & coding
- Staff inexperience & turnover
- Truncated testing
- Botched deployments

Failure avoidance practices
- Feasibility analysis
- Mission & business analysis
- Acquisition management
- Project & risk management
- Baseline management
- Technical risk measurement
- Contractual personnel clauses
- Quality management
- Acceptance management

Software measurement
Software quality evaluation of 108 Federal systems regarding factors affecting operational and cost risk

- **Too high quality**: 5
- **Quality is good**: 17
- **Needs minor improvement**: 34
- **Needs major improvement**: 46
- **Outside range**: 6

John Marien, MITRE, 2019
What Is CISQ?

CISQ Co-founders

Dr. Paul Nielsen, CEO

Dr. Richard Soley, CEO

Carnegie Mellon Software Engineering Institute

Develop specifications for automatable measures of software systems

Gain approval as OMG standards

Fast-track to ISO

CISQ Sponsors

CISQ Partners
The CISQ Security measure (and others) can be used in numerous processes of the NIST Cybersecurity Framework. Some examples:

- **Empirical software security risk tolerance thresholds**
- **Contractual SLAs and audits for software security**
- **Evaluation of software assets for security weaknesses**
- **Continual improvement of software security**
- **Periodic scans for software weaknesses**
- **Software security and weakness data are shared**
- **Security weaknesses are identified and mitigated**

The CISQ structural quality measures play an important requirements and verification role for ‘Build Security In’ approaches to cybersecurity.
Trustworthy Systems Manifesto

1. Engineering discipline in product and process
2. Quality assurance to risk tolerance thresholds
3. Traceable properties of system components
4. Proactive defense of the system and its data
5. Resilient and safe operations

www.it-cisq.org
Free membership
Summary

• CISQ measures provide industry standard quantification of software reliability, security, and cost risk

• CISQ measures are designed for automation and are supported by an ecosystem of vendors

• CISQ measures integrate seamlessly with modern agile processes, ISO standards, and NIST frameworks

• CISQ measures are already mandated in some government and industry acquisitions and can be written into policy