Trustworthy Systems Manifesto

Executive Policy Governing Cyber Risk to the Mission and Business

Dr. Bill Curtis
Executive Director, CISQ

CISQ
Consortium for IT Software Quality

International Standards for Automating Software Size and Structural Quality Measurement

TRUSTWORTHY SYSTEMS MANIFESTO

We hold these truths to be self-evident
The 9-Digit Glitch

9-Digit Glitches

now affect

Board of Directors
CEO, COO, CFO
Business VPs
Corporate Auditors
CIO

accountable for

Governance
Risk management
Business Continuity
Brand protection
Customer experience

Evaluate Application Risk with CISQ Measures
What Is CISQ?

CISQ is chartered to specify measures of software size and quality that can be automated from source code, and promote them through OMG and other international standards organizations.

Co-founders
- Paul Nielsen
- Richard Soley

CISQ Sponsors
- Cognizant
- SYNPYSS
- TECH Mahindra
- SHPI
- CAST
- CGI
- NORTHROP GRUMMAN

CISQ Partners
- Gartner
- FORRESTER
- IAAC
- IAO
- TECHWELL
- MAKING SOFTWARE BETTER
Deploying CISQ Measures

CISQ measures → OMG standards → ISO standards

Federal IT Policy

Corporate IT Policy

Regulations
- Sec. & Exch. Com.
- State of Texas

System acquisition
- US State Dept.
- Gen. Serv. Admin.

Third party Contracts

Benchmarks

US State Dept.
Gen. Serv. Admin.
The Era of 9-Digit Glitches

In summary, the cost of poor-quality software in the US in 2018 is approximately $2.84 trillion.
Current Focus Is on Developers, Not Enterprises

Manifesto for Agile Software Development

We are uncovering better ways of developing software by doing it and helping others do it. Through this work we have come to value:

- Individuals and interactions over processes and tools
- Working software over comprehensive documentation
- Customer collaboration over contract negotiation
- Responding to change over following a plan

That is, while there is value in the items on the right, we value the items on the left more.

The Rugged Manifesto

I am rugged and, more importantly, my code is rugged.
I recognize that software has become a foundation of our modern world.
I recognize the awesome responsibility that comes with this foundational role.
I recognize that my code will be used in ways I cannot anticipate, in ways it was not designed, and for longer than it was ever intended.
I recognize that my code will be attacked by talented and persistent adversaries who threaten our physical, economic and national security.

I recognize these things – and I choose to be rugged.

I am rugged because I refuse to be a source of vulnerability or weakness.
I am rugged because I assure my code will support its mission.
I am rugged because my code can face these challenges and persist in spite of them.
I am rugged, not because it is easy, but because it is necessary and I am up for the challenge.
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
The principles and practices of software engineering must predominate other considerations in developing software-intensive systems.

Trustworthy systems do not emerge from haphazard development and deployment processes.

The shorter the time, the greater the need for process discipline.

Developers and operators must be supplemented by automated technologies that can reduce complexity and improve their visibility into systems and operations.

Organizations must ensure that developers have the knowledge and skills needed to build and deploy trustworthy systems.
1 — Executives must determine the risk that can be tolerated from each business or mission critical system

2 — Quality assurance must ensure the system operates within risk tolerance thresholds

3 — Executives must establish policy that critical systems have evidence they can perform within risk thresholds before being released to operations

4 — Executives must enforce that time be devoted to remediating high priority defects
3 — Traceable Properties of System Components

1 — Developing modern software-intensive systems requires managing a supply chain of component sources

2 — Evidence of provenance and trustworthiness should be carried forward with components and shared across the supply chain
4 — Proactive Defense of the System and Its Data

1 — Protection of the system and its data from malicious actors requires several layers of defense

2 — System behavior should be continuously monitored to detect suspicious actions and data movements

3 — Security practices must also cover the behavior of authorized system users to ensure system defenses are not circumvented
Resilient and Safe Operations

TRUSTWORTHY SYSTEMS MANIFESTO

We hold these truths to be self-evident

1. To sustain the business or mission, systems must be able to continue operations in the face of unexpected events, or if interrupted, recover their operations efficiently.

2. Failsafe properties of software-intensive systems should be designed in and verified.
Charter of Trust
For a secure digital world

The digital world is changing everything. Critical management and legacy systems are being replaced by emerging technologies. Digital transformation is being enabled by the Internet of Things and inserting AI into a connected global market.

As a result, these changes are impacting or have an impact on the risks and opportunities, the role of experts in the field of cybersecurity is inalienable. Cyberattacks target systems that sustain our homes, hospitals, factories, grids, and infrastructure. The potential risk of interference can be enormous. Criminals and malicious actors need to be protected from cyber and physical attacks.

Cybersecurity is now more than a methodology or a string of processes, it’s a factor that’s crucial to the success of the digital economy. Companies and organizations need to ensure that their digital infrastructure is safe and secure, otherwise they won’t achieve their digital transformation. Digitalization and cybersecurity must go hand-in-hand.

In order to bring about a continuous increase in the market as well as threats from the central core, companies and governments must join forces and take decisive action. The sooner we make every effort to protect the data and assets of individuals and businesses, prevent damages from people, businesses, and enterprises, and build a viable business for society in a connected and digital world.

Our principles:

1. Ownership of cyber and IT security | Anchor the responsibility for cybersecurity at the highest government and business levels by designating specific ministries and CISOs. Establish clear measures and targets as well as the right mindset throughout organizations – “it's everyone’s task.”

2. Responsibility throughout the digital supply chain | Companies – and if necessary – governments must establish risk-based rules that ensure adequate protection across all IoT layers with clearly defined and mandatory requirements. Ensure confidentiality, authenticity, integrity, and availability by setting baseline standards, such as
   - Identity and access management: Connected devices must have secure identities and safeguarding measures that only allow authorized users and devices to use them.
   - Encryption: Connected devices must ensure confidentiality for data storage and transmission purposes wherever appropriate.
   - Continuous protection: Companies must offer updates, upgrades, and patches throughout a reasonable lifecycle for their products, systems, and services via a secure update mechanism.

3. Security by default | Adopt the highest appropriate level of security and data protection and ensure that it is preconfigured into the design of products, functionalities, processes, technologies, operations, architectures, and business models.

4. User-centricity | Serve as a trusted partner throughout a reasonable lifecycle, providing products, systems, and services as well as guidance based on the customer’s cybersecurity needs, impacts, and risks.

5. Innovation and co-creation | Combine domain knowledge and deepen a joint understanding between firms and policymakers of cybersecurity requirements and rules in order to continuously innovate and adapt cybersecurity measures to new threats; drive and encourage i.e. contractual Public Private Partnerships.

6. Education | Include dedicated cybersecurity courses in school curricula – as degree courses in universities, professional education, and training – in order to lead the transformation of skills and job profiles needed for the future.

7. Certification for critical infrastructure and solutions | Companies – and if necessary – governments establish mandatory independent third-party certifications (based on future-proof definitions, where life and limb is at risk in particular) for critical infrastructure as well as critical IoT solutions.

8. Transparency and response | Participate in an industrial cybersecurity network in order to share new insights, information on incidents et al.; report incidents beyond today’s practice, which is focusing on critical infrastructure.

9. Regulatory framework | Promote multilateral collaborations in regulation and standardization to set a level playing field matching the global reach of the WTO; inclusion of rules for cybersecurity into Free Trade Agreements (FTAs).

10. Joint initiatives | Drive joint initiatives, including all relevant stakeholders, in order to implement the above principles in the various parts of the digital world without undue delay.

© 2018 Consortium for IT Software Quality (CISQ) www.it-cisq.org

Charter of Trust
For a secure digital world

Access Manifesto

Read Manifesto

Sign Manifesto

TRUSTWORTHY SYSTEMS MANIFESTO

As a greater portion of mission, business, and safety-critical functionality is committed to software-intensive systems, these systems become one of, if not the largest source of risk to enterprises and their customers. Since corporate executives are ultimately responsible for managing this risk, we establish the following principles to govern system development and deployment:

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

These principles are developed and practiced within their organizations to implement these principles, and to encourage others to adopt these organizations.

This manifesto is developed and maintained by the Consortium for IT Software Quality (CISQ), a not-for-profit IT standards organization. CISQ is a member-driven, not-for-profit IT standards organization. CISQ is dedicated to advancing the trustworthiness of software-intensive systems by producing standards for automating the measurement of size and structural quality from software source code. CISQ’s community outreach activities to spread awareness and promote the trustworthiness of software-intensive systems.

© 2018 Consortium for IT Software Quality (CISQ) www.it-cisq.org
CISQ Membership Is Free — www.it-cisq.org

Over 2000 individual members from large software-intensive organizations:

- Accenture
- AT&T
- Amazon
- Infosys
- Bosch
- Aetna
- Booz Allen Hamilton
- Credit Suisse
- John Deere
- ISG
- Boeing
- Amgen
- Allianz
- Gartner
- IAO
- Citi
- Capital One
- Capgemini
- Dell
- FedEx
- Discovery Health
- CenturyLink
- MITRE
- Barclays
- Huawei
- NHS
- Autodesk
- Discovery Health