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

The Era of 9-Digit Glitches

Consortium for IT Software Quality

Forbes Billionaires Innovation Leadership Money Consumer Industry

73,101 views | Jan 17, 2016, 11:01am

Cyber Crime Costs Projected To Reach $2 Trillion by 2019

Steve Morgan Contributor ⓘ
I write about the business of cybersecurity.

Photographer: Ken Cedeno/Bloomberg News.

'Crime wave' is an understatement when you consider the costs that businesses are suffering as a result of cyber crime. 'Epidemic' is more like it. IBM Corp.'s Chairman, CEO and President, Ginni Rometty, recently said that cyber crime may be the greatest threat to every company in the world.

Veek

Security

e Costs

s in Ne

ecovery pl

The Cost of Poor Quality Software in the US: A 201 ort

apital & Careers

Data Security

600M'

Search

at is the

is $5,600

With Risk

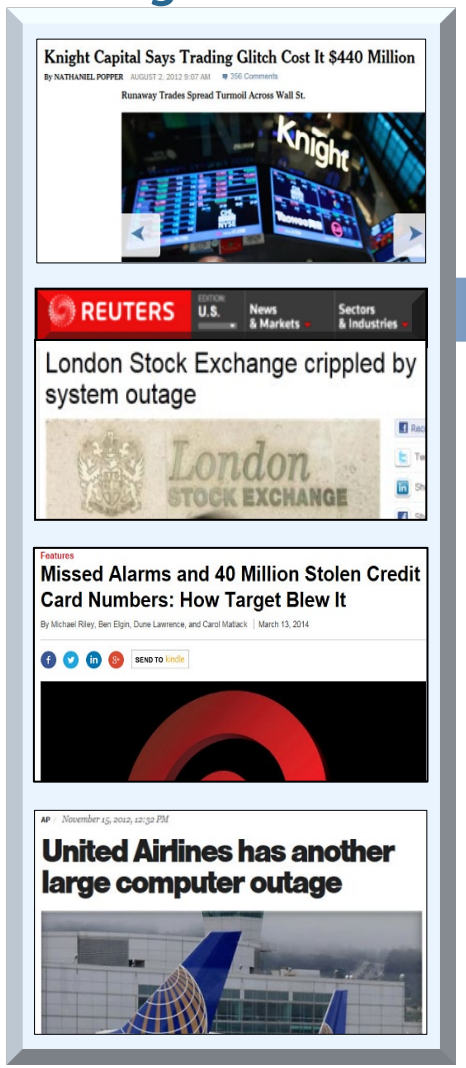
In summary, the cost of poor-quality software in the US in 2018 is approximately $2.84 trillion

CISQ

Consortium for IT Software Quality

Responsibility Has Shifted Above IT / Engineering

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
- Product liability

Evaluate System Risk with CISQ Measures

What Is CISQ ?

Carnegie Mellon Software Engineering Institute

OBJECT MANAGEMENT GROUP®

Co-founders

Paul Nielsen → **CISQ** ← **Richard Soley**

CISQ

OMG Special Interest Group

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

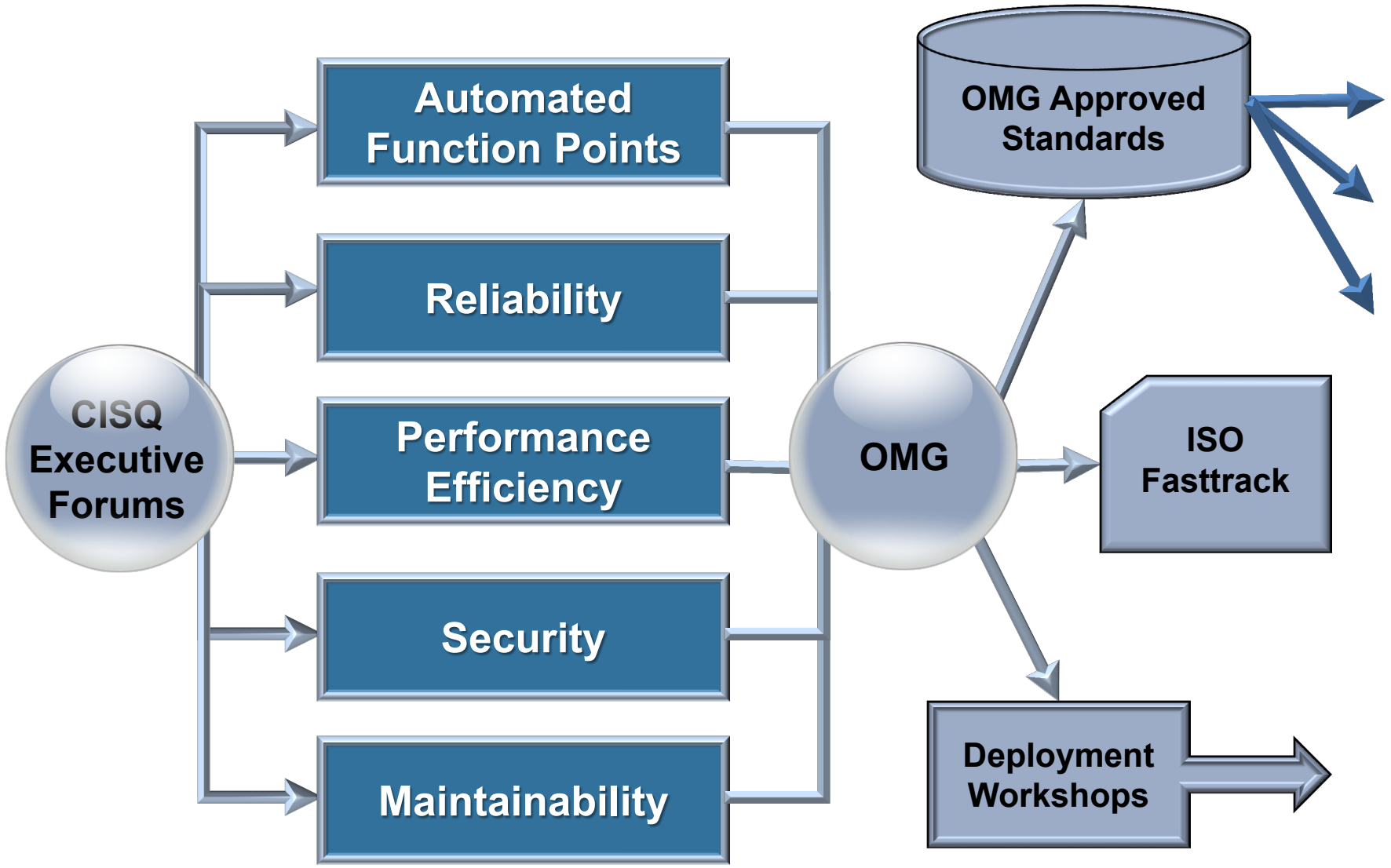
CISQ Sponsors

Cognizant, SYNOPSYS®, Tech Mahindra, SHPI, CAST, CGI, NORTHROP GRUMMAN

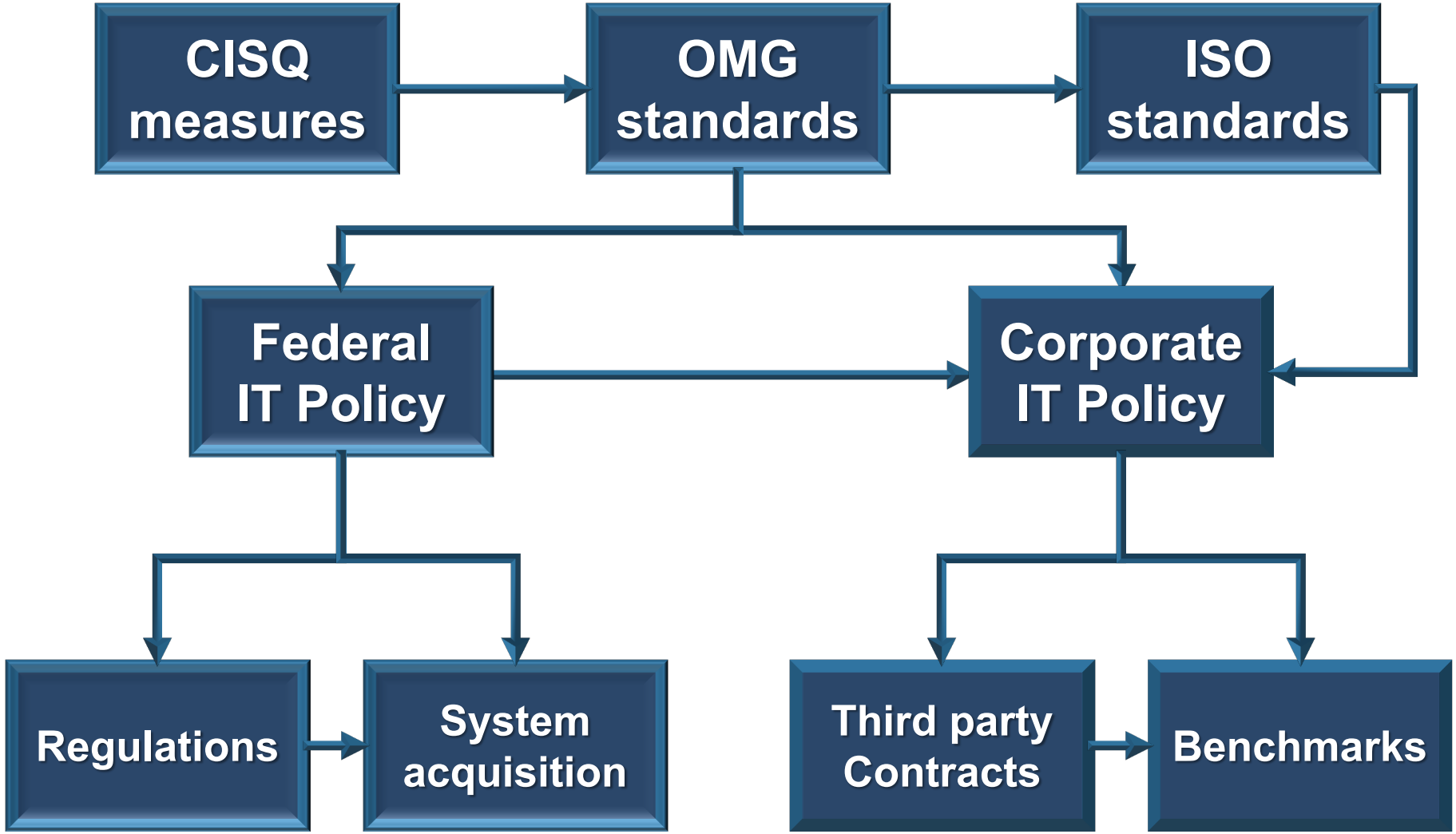
CISQ Partners

Gartner, QuEST FORUM, FORRESTER®, IAOP, ITAAC, TECHWELL, MAKING SOFTWARE BETTER

CISQ/OMG Standards Process



Deploying CISQ Measures



Current Focus Is on Developers, Not Enterprises

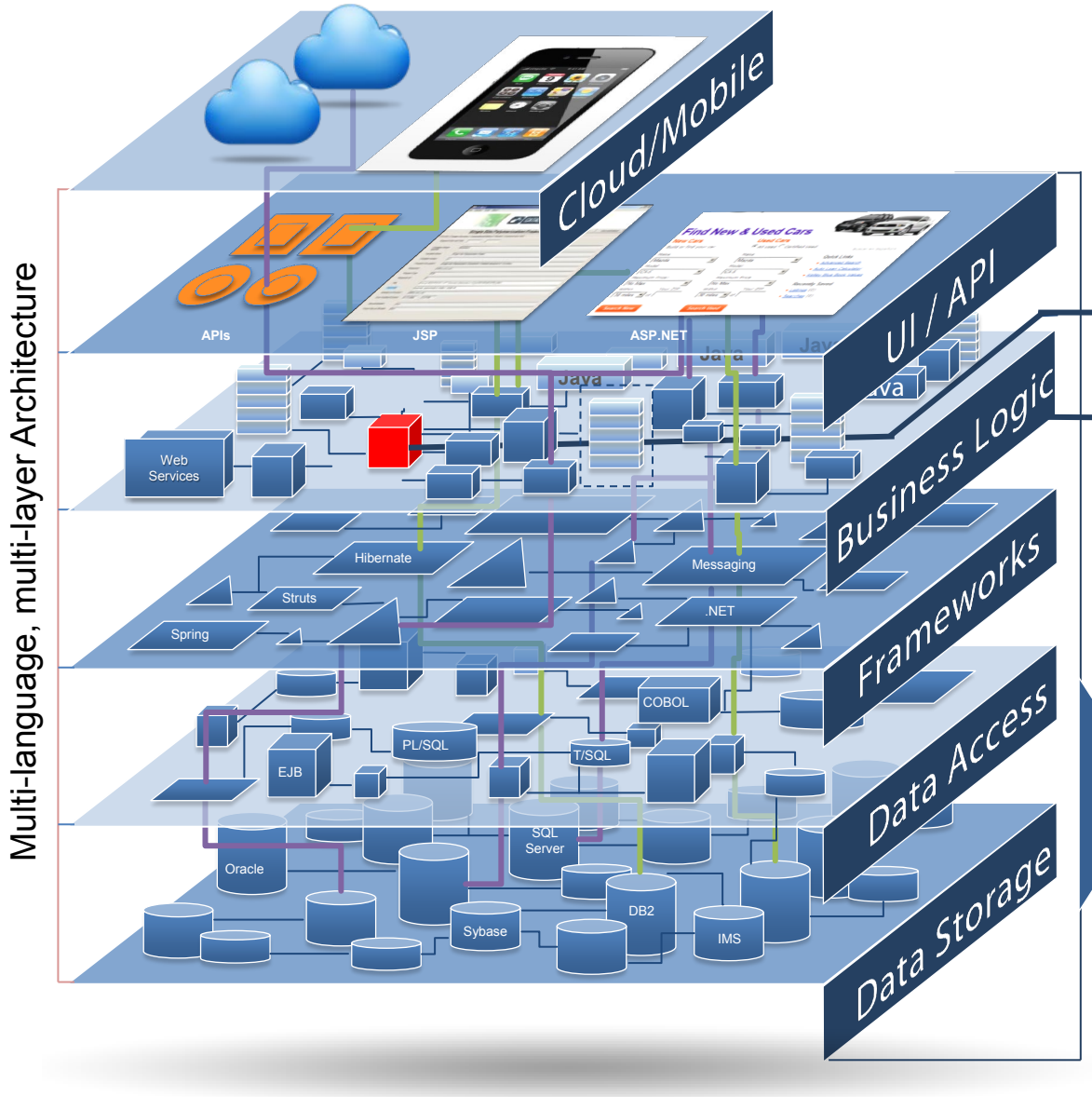
The Rugged Manifesto

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.

Modern Apps Are a Technology Stack



1 Unit Level

- Code style & layout
- Expression complexity
- Code documentation
- Class or program design
- Basic coding standards
- Developer level

2 Technology Level

- Single language/technology layer
- Intra-technology architecture
- Intra-layer dependencies
- Inter-program invocation
- Security vulnerabilities
- Development team level

3 System Level

- Multiple languages
- Architectural compliance
- Risk propagation
- Application security
- Resiliency checks
- Transaction integrity
- Function points
- Integration quality
- Data access control
- SDK versioning
- Calibration across technologies
- IT organization level

Need for a New Manifesto

Existing manifestos

- focused on individuals (and teams), not organizations
- under-emphasized quality and operational risk
- were more about coding than software engineering
- failed to represent management's responsibilities
- did not create dialogue among responsible parties

Executives own the risk,
But are not tech experts

↓

Executives need guidance on how to reduce risk and policies to apply in IT/Eng

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

1 — Engineering Discipline in Process and Product

1 — The principles and practices of software engineering must predominate other considerations in developing software-intensive systems

2 — Trustworthy systems do not emerge from haphazard development and deployment processes

3 — The shorter the time, the greater the need for process discipline

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

5 — Organizations must ensure that developers have the knowledge and skills needed to build and deploy trustworthy systems.

2 — Quality Assurance to Risk Tolerance Thresholds

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 — Track and patch known vulnerabilities

4 — Security practices must also cover the behavior of authorized system users to ensure system defenses are not circumvented

5 — Resilient and Safe Operations

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

NIST, ISO, & IIC Structure of Trustworthiness

Trustworthy Systems Manifesto

NIST, ISO, IIC Trustworthiness

ISO/IEC JTC1 SC41

- Safety
- Reliability
- Security
- Resilience
- Privacy

1. 1 – Eng. discipline in process & product
2. 2 – QA to risk tolerance thresholds
3. 3 – Traceable properties of components
4. 4 – Proactive defense of system & data
5. 5 – Resilient & safe operations

Charter of Trust

Consortium for IT Software Quality

https://www.siemens.com/content/dam/webassetpool/mam/tag-siemens-com/smdb/corporate-core/topic-areas/digitalization/cybersecurity/shi-13378-cot-dok-narrative-online-2018-02-13-sbi-en.pdf

Our principles

1 Ownership of cyber and IT security | Anchor the responsibility for cybersecurity at the highest governmental and business levels by designating specific ministries and CISOs. Establish clear measures and targets as well as the right mindset throughout organizations – "It is 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 know-how 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.a. contractual Public Private Partnerships.

6 Education | Include dedicated cybersecurity courses in school curricula – as degree courses in universities, professional education, and trainings – 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.

Use the Manifesto to Start Dialogues

Executive Team

business needs

Policies

risk thresholds

CIO

CISO

Vendor Mgt.

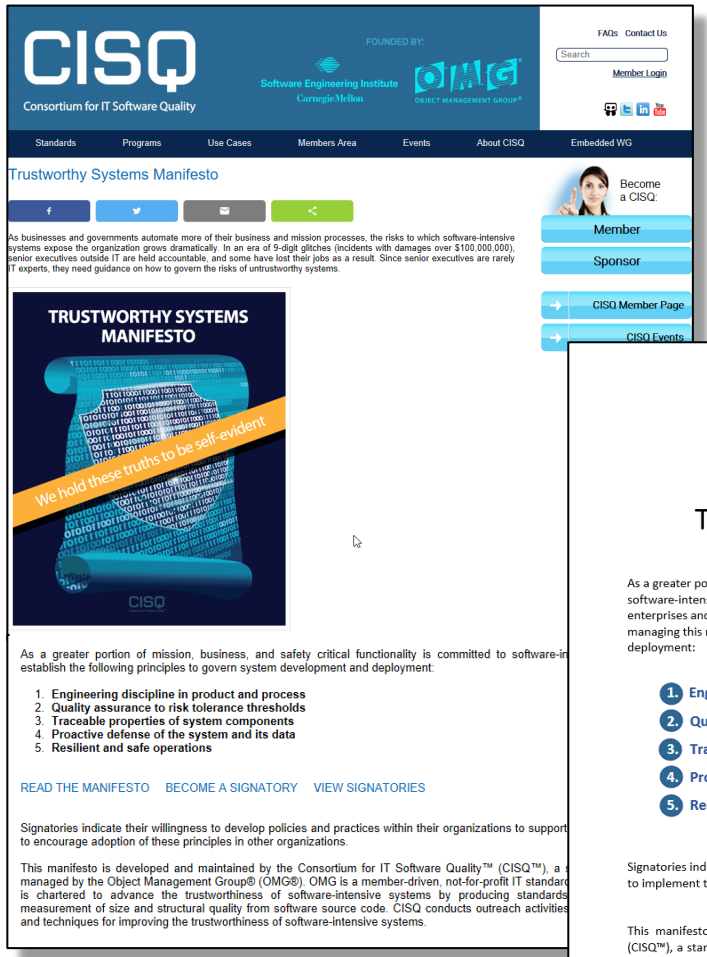
Development

QA

Operations

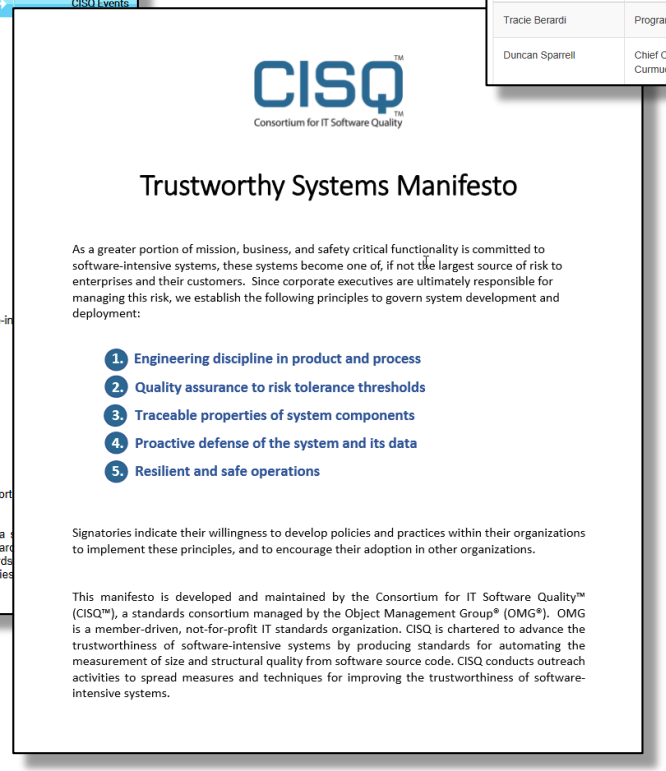
Audit

Sign the Manifesto — it-cisq.org/trustworthy-systems-manifesto

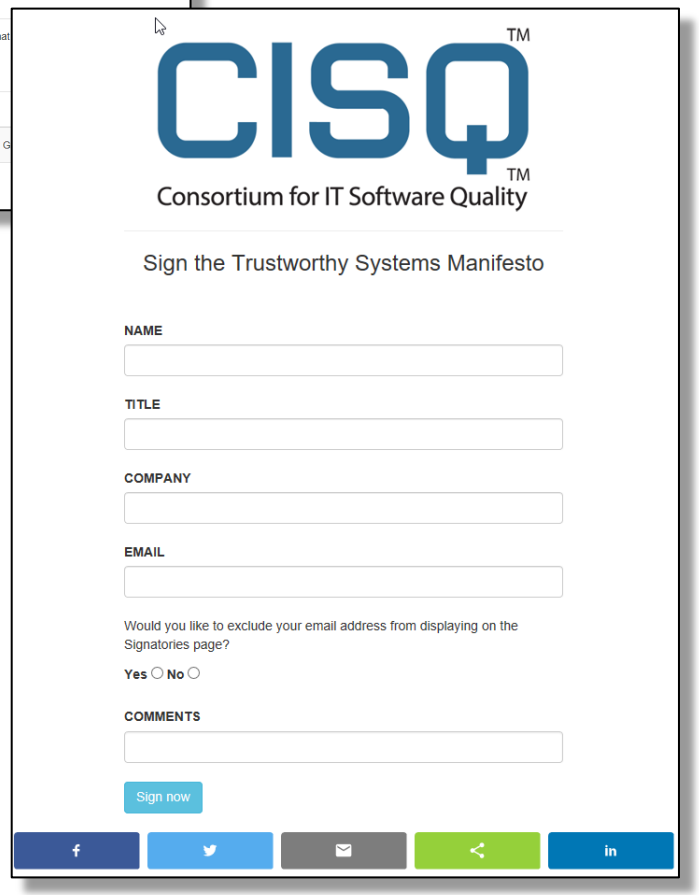


Access Manifesto

Review Signatories



Read Manifesto



Sign Manifesto

CISQ Membership Is Free — www.it-cisq.org

Over 2000 individual members from large software-intensive organizations:

accenture, U.S. Department of Homeland Security, European Union, IBM, AXA, at&t, amazon, Infosys, BOSCH, ISG, BOEING, aetna, John Deere, Booz | Allen | Hamilton, Credit Suisse, Duke Energy, IAOP, Allianz, Gartner, Atos, citi, Capital One, DreamWorks Animation SKG, Huawei, Capgemini, DELL, FedEx, Discovery Health, ca technologies, DCG, CISCO, Fidelity Investments, HCL, CenturyLink, MITRE, BARCLAYS