

# Trustworthy Systems Manifesto

Executive Policy Governing Cyber  
Risk to the Mission and Business

**Dr. Bill Curtis**

Executive Director, CISQ

**CISQ**

International Standards for  
Automating Software Size and  
Structural Quality Measurement

Consortium for IT Software Quality

## TRUSTWORTHY SYSTEMS MANIFESTO



We hold these truths to be self-evident

**CISQ**  
Consortium for IT Software Quality

## 9-Digit Glitches

**Knight Capital Says Trading Glitch Cost It \$440 Million**  
By NATHANIEL POPPER AUGUST 2, 2012 9:07 AM 350 Comments  
Runaway Trades Spread Turmoil Across Wall St.

**REUTERS** U.S. News & Markets Sectors & Industries  
**London Stock Exchange crippled by system outage**

**Features**  
**Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It**  
By Michael Riley, Ben Elgin, Dune Lawrence, and Carol Matlack | March 13, 2014

**AP** November 15, 2010, 12:39 PM  
**United Airlines has another large computer outage**

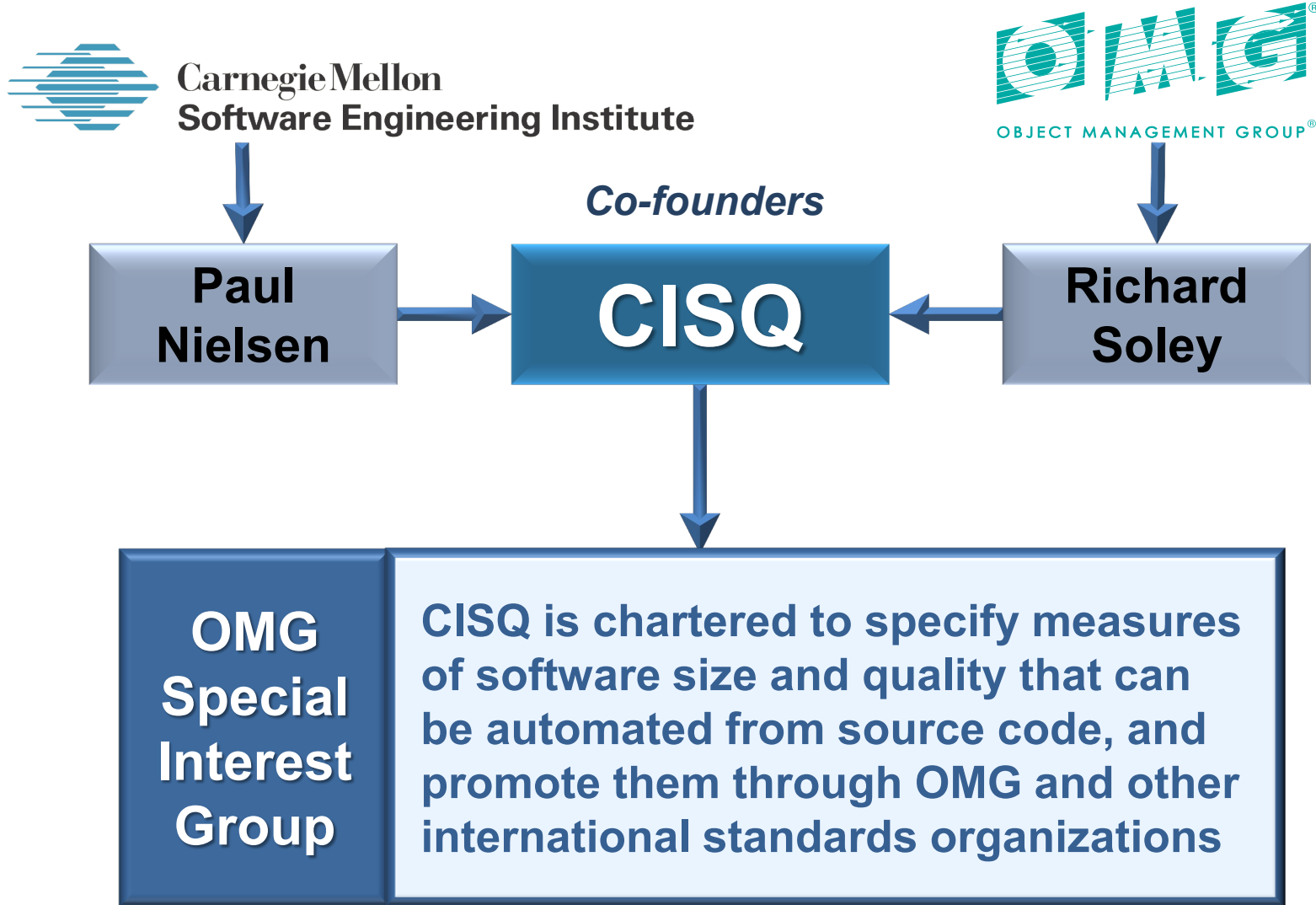
now affect

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

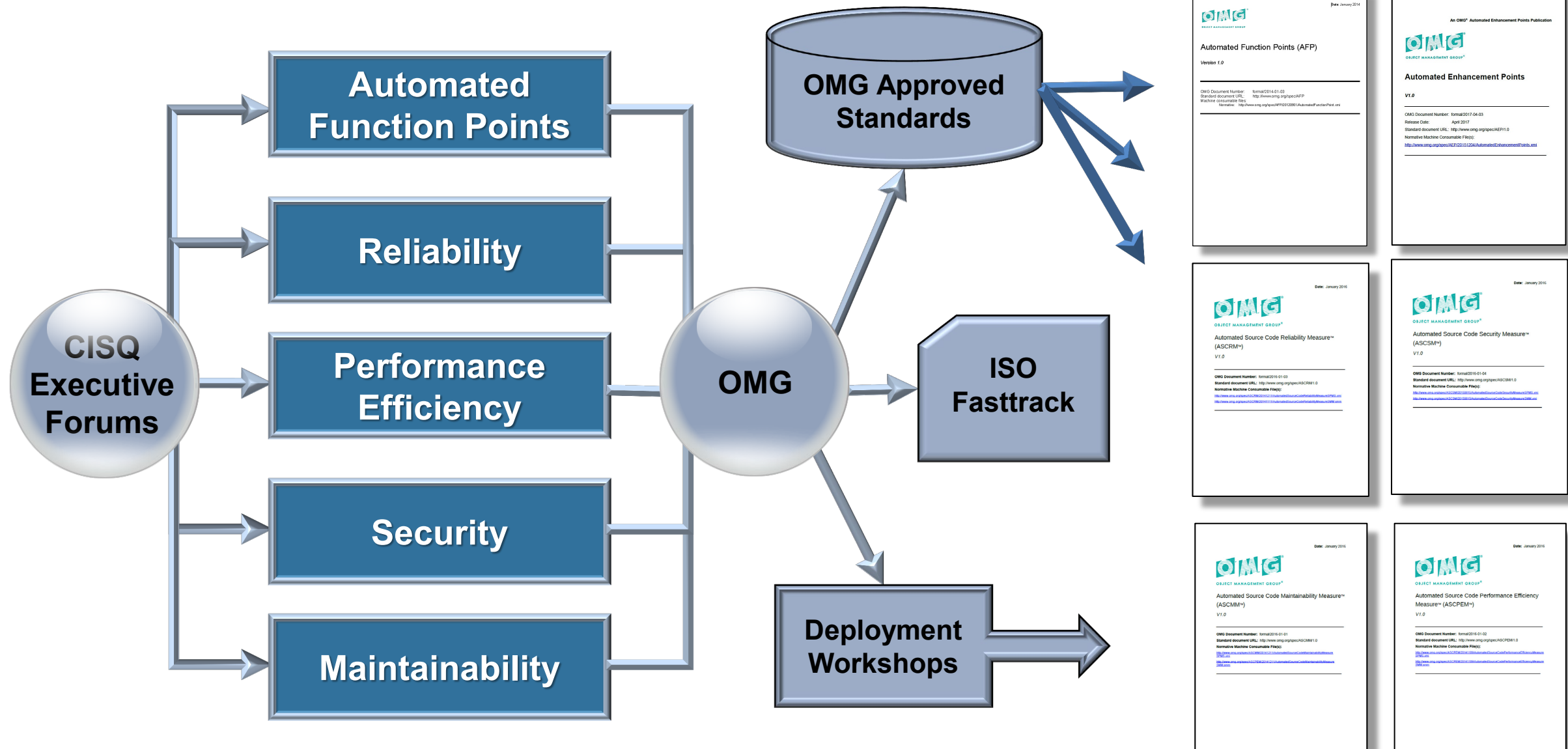


## CISQ Sponsors

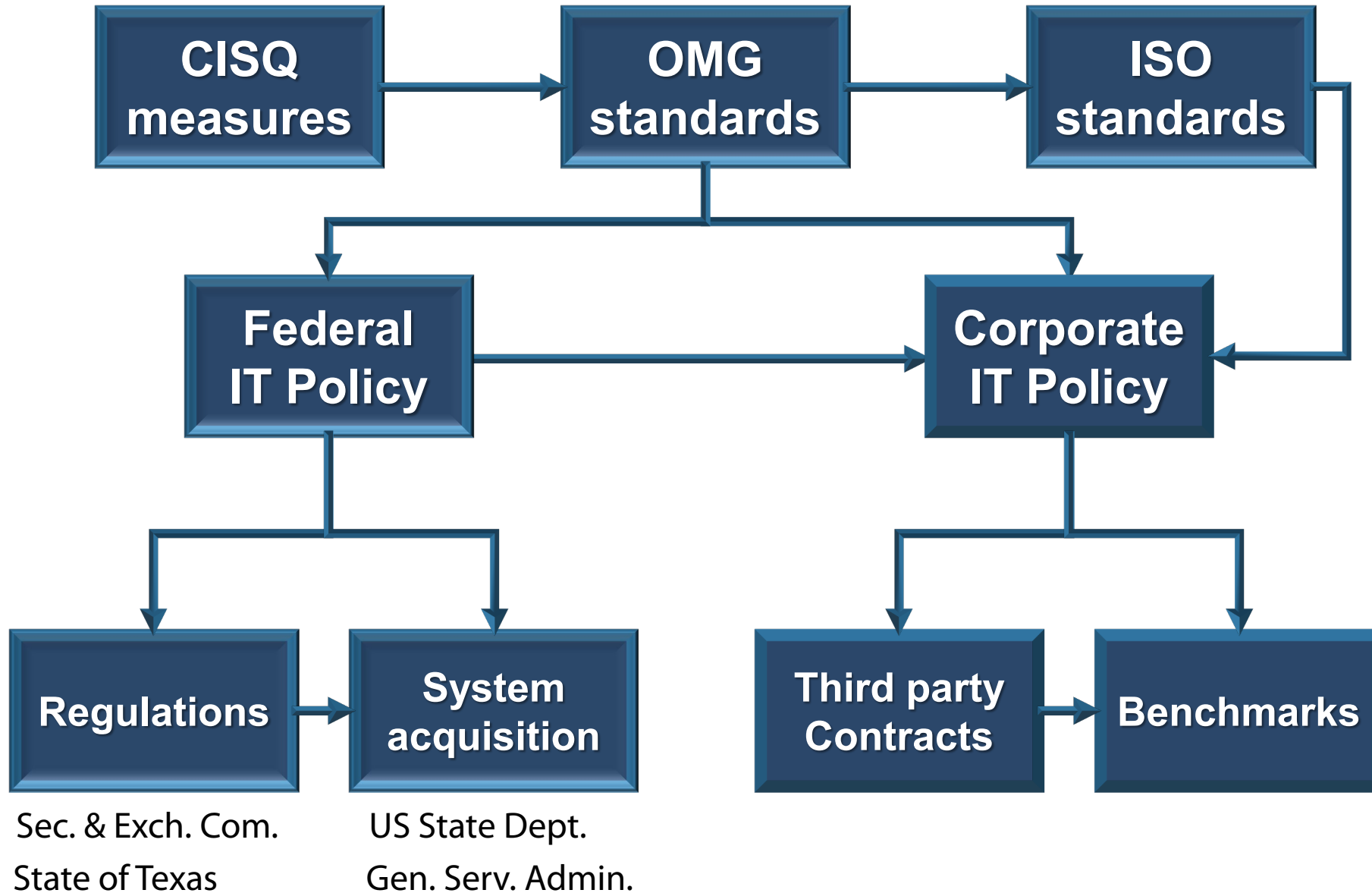


## CISQ Partners





# Deploying CISQ Measures





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.

### Week

Security

### e Costs

s in No.  
recovery pl

The Cost of Poor Quality Software in the US:  
A 2018 Report

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

## 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.



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



## TRUSTWORTHY SYSTEMS MANIFESTO

We hold these truths to be self-evident

- 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.

## TRUSTWORTHY SYSTEMS MANIFESTO

We hold these truths to be self-evident

- 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



## TRUSTWORTHY SYSTEMS MANIFESTO

We hold these truths to be self-evident

- 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



## TRUSTWORTHY SYSTEMS MANIFESTO

We hold these truths to be self-evident

- 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

## 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



Charter of Trust

## Charter of Trust For a secure digital world

**The digital world is changing everything.** Artificial intelligence and big data analytics are revolutionizing our decision-making; billions of devices are being connected by the Internet of Things and interacting on an entirely new level and scale.

As much as these advances are improving our lives and economies, the risk of exposure to malicious cyber-attacks is also growing dramatically. Failure to protect the systems that control our homes, hospitals, factories, grids, and virtually all of our infrastructure could have devastating consequences. **Democratic and economic values need to be protected from cyber and hybrid threats.**

Cybersecurity is and has to be more than a seatbelt or an airbag here; it's a factor that's crucial to the success of the digital economy. People and organizations need to trust that their digital technologies are safe and secure; otherwise they won't embrace the digital transformation. **Digitalization and cybersecurity must evolve hand in hand.**

In order to keep pace with continuous advances in the market as well as threats from the criminal world, companies and governments must join forces and take decisive action. This means making every effort to protect the data and assets of individuals and businesses; prevent damage from people, businesses, and infrastructures; and build a reliable basis for trust in a connected and digital world.

Hedging the all-encompassing impact of digitalization and cybersecurity and creating a holistic basis of trust can't be achieved by a single company or entity; it must be the result of close collaborations on all levels. **In this charter, the signing partners outline the key principles we consider essential for establishing a new charter of trust between society, politics, business partners, and customers.**



### 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.



**Trustworthy Systems Manifesto**

As businesses and governments automate more of their business and mission processes, the risks to which software-intensive systems expose the organization grows dramatically. In an era of 8-digit glitches (incidents with damages over \$100,000,000), senior executives outside IT are held accountable, and some have lost their jobs as a result. Since senior executives are rarely IT experts, they need guidance on how to govern the risks of untrustworthy systems.

**TRUSTWORTHY SYSTEMS MANIFESTO**

We hold these truths to be self-evident

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

Signatories indicate their willingness to develop policies and practices within their organizations to support to encourage adoption of these principles in other organizations.

This manifesto is developed and maintained by the Consortium for IT Software Quality™ (CISQ™), a standards consortium managed by the Object Management Group® (OMG®). OMG is a member-driven, not-for-profit IT standards organization. CISQ is chartered to advance the trustworthiness of software-intensive systems by producing standards for automating the measurement of size and structural quality from software source code. CISQ conducts outreach activities and techniques for improving the trustworthiness of software-intensive systems.

## Access 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

Signatories indicate their willingness to develop policies and practices within their organizations to implement these principles, and to encourage their adoption in other organizations.

This manifesto is developed and maintained by the Consortium for IT Software Quality™ (CISQ™), a standards consortium managed by the Object Management Group® (OMG®). OMG is a member-driven, not-for-profit IT standards organization. CISQ is chartered to advance the trustworthiness of software-intensive systems by producing standards for automating the measurement of size and structural quality from software source code. CISQ conducts outreach activities to spread measures and techniques for improving the trustworthiness of software-intensive systems.

## Read Manifesto

**TRUSTWORTHY SYSTEMS MANIFESTO**

NAME	TITLE	COMPANY	EMAIL
Tracie Berardi	Program Manager	CISQ	tracie(at)omg.org
Duncan Sparrell	Chief Cyber Curmudgeon	sFractal Consulting	

## Review Signatories

**Sign the Trustworthy Systems Manifesto**

NAME

TITLE

COMPANY

EMAIL

Would you like to exclude your email address from displaying on the Signatories page?  
Yes  No

COMMENTS

## Sign Manifesto

Over 2000 individual members from large software-intensive organizations:

