Role Of Code Standards in Business Risk Mitigation

Dave Norton
Dark Matter Advisory

Advisor
Consortium for Information & Software Quality

david.norton@it-cisq.org

Finance Cyber Incidents in the UK, Up 1087% Increase Year on Year

Root Cause	2019	2018	% of Incidents
Hardware and software issues	157	64	19%
Change management	146	53	18%
Third-party failure	174	79	21%
Cyber-attack - Distributed denial of service (DDoS)	10	2	1%
Cyber-attack - Malware	16	5	2%
Cyber-attack - Ransomware	19	0	2%
Cyber-attack - Phishing or other compromise of credentials	48	29	6%
To be confirmed	93	82	11%
Human error	47	24	6%
Process/control failure	45	17	5%
Failure to manage adequate IT capacity	25	4	3%
External factors	17	3	2%
Theft	11	3	1%
Cause unknown	11	5	1%
	819	**370**	**100%**

- 21%, are related to third-party failure, i.e., systems the reporting organization did not control.
- However, many of the other incidents had their origins in third-party developed software now owned by the reporting organization.

CISQ
Consortium for Information & Software Quality™

Even CEOS Are Paying The Price For Poor IT Quality

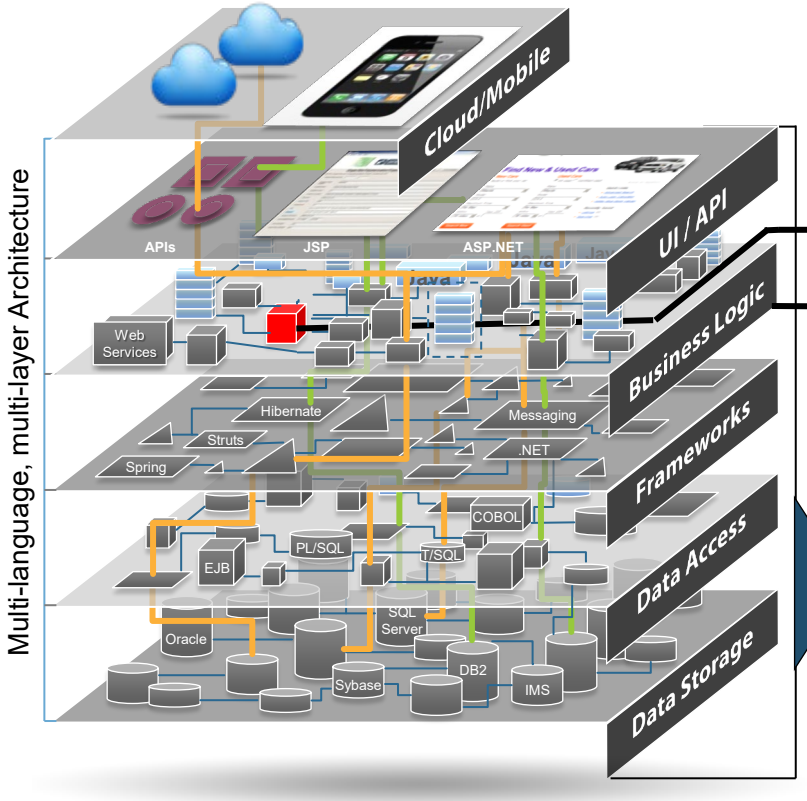
British Airways' chief executive Álex Cruz says he will not resign despite a "catastrophic" IT system failure that grounded scores of flights

Paul Pester forced to step down as CEO of TSB after the disruption caused to millions of customers by the bank's very public failed IT upgrade

Former Equifax CEO Richard Smith says he is "deeply sorry" for the security breach in which sensitive personal information of as many as 143 million Americans was compromised

CISQ
Consortium for Information & Software Quality™

Complex Technology Stack



Technology Stack

1 Unit Level

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

2 Technology Level

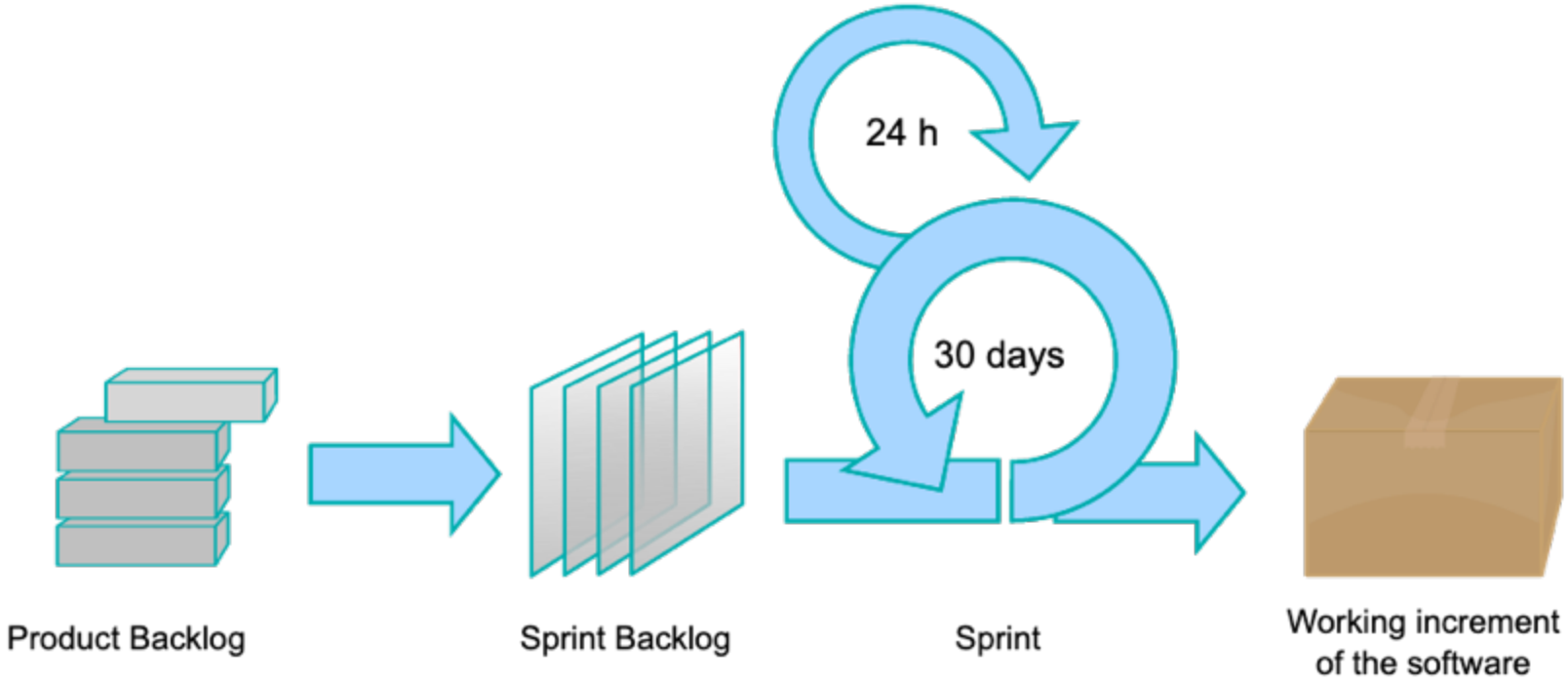
- Single language/technology layer
- Intra-technology architecture
- Intra-layer dependencies
- Inter-program invocation
- Security vulnerabilities
- Development team level

3 System Level

- Integration quality
- Architectural compliance
- Risk propagation
- Application security
- Resiliency checks
- Transaction integrity
- Function point,
- Effort estimation
- Data access control
- SDK versioning
- Calibration across technologies
- IT organization level

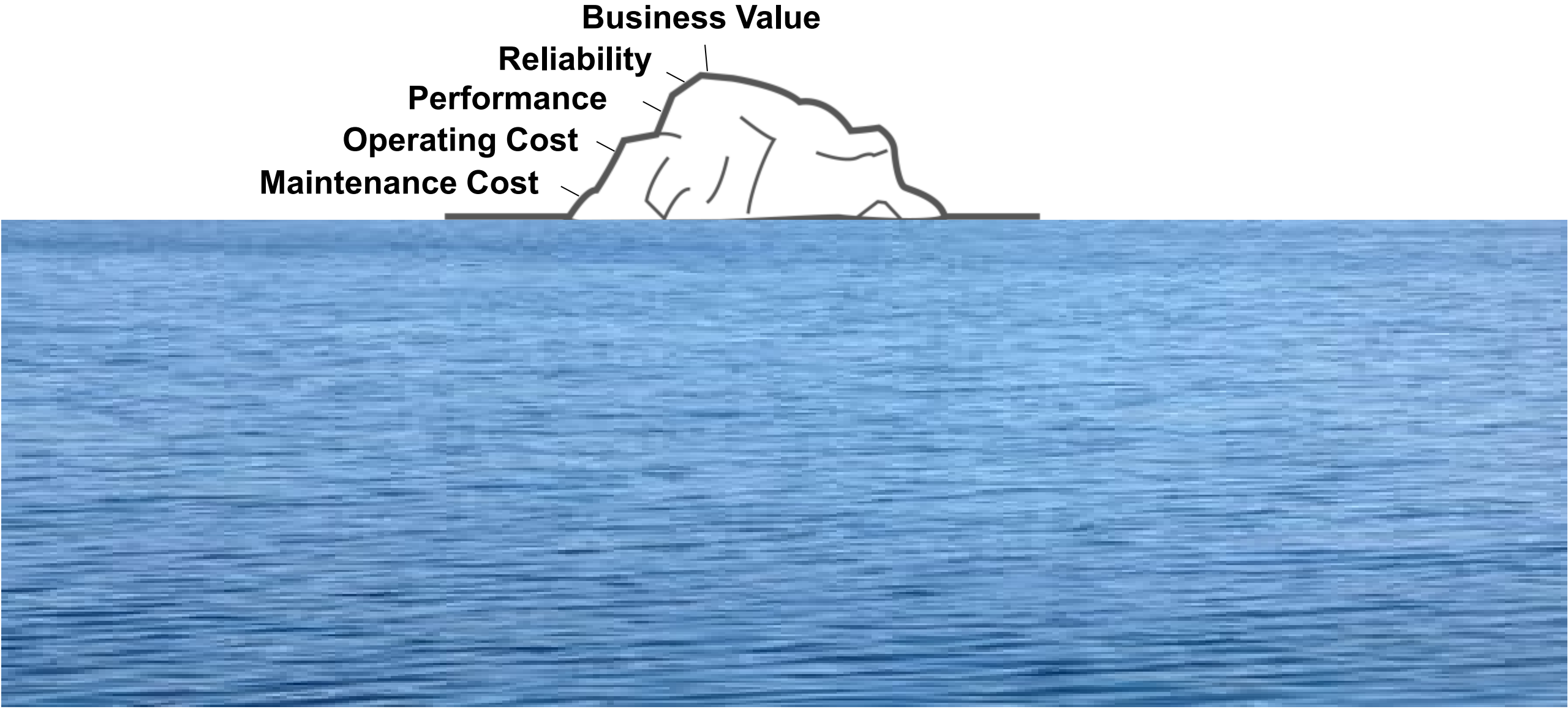
CISQ
Consortium for Information & Software Quality™

We Want More Productivity, But at What Cost?

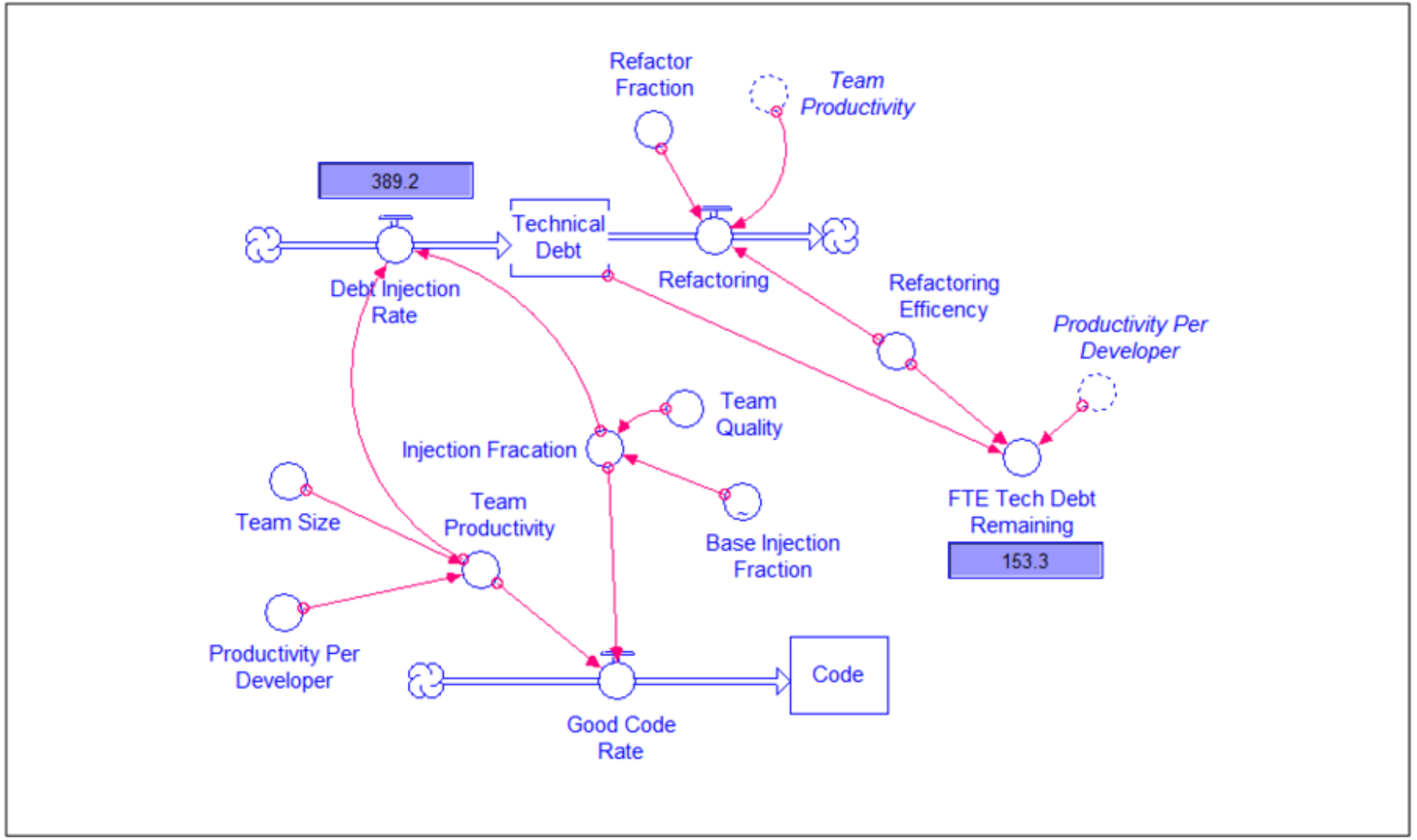


Everyone wants faster time to market, but few want to hear about the risks

Increasing Technical Debt



Simulation Of 120 Day Project



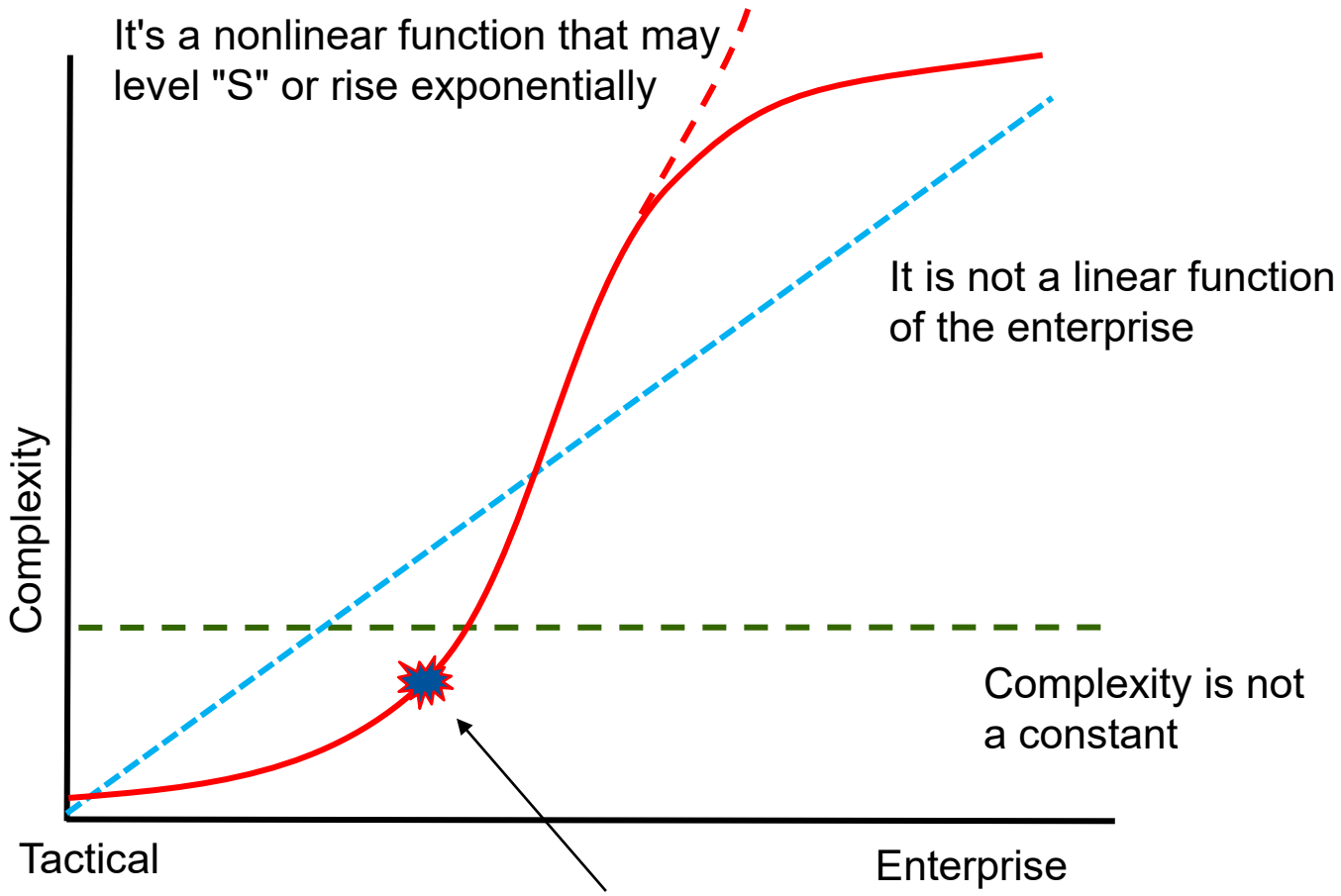
https://forio.com/simulate/dpnorton66/tech-debt-v3/simulation/#

Example After 120 Day Project – Average Team

		Refactoring	FTE Tech Debt	Refactoring Cost	
Team Size	Inject Rate	Rate	Days Left	At $240	At $1040
5	10 - 25%	10%	63.2	$15,168	$65,728
10	10 - 25%	10%	126.4	$30,336	$131,456
20	10 - 25%	10%	252.8	$60,672	$262,912

https://forio.com/simulate/dpnorton66/tech-debt-v3/simulation/#

Microservices and API's Can Accelerate Architecture Debt and Complexity

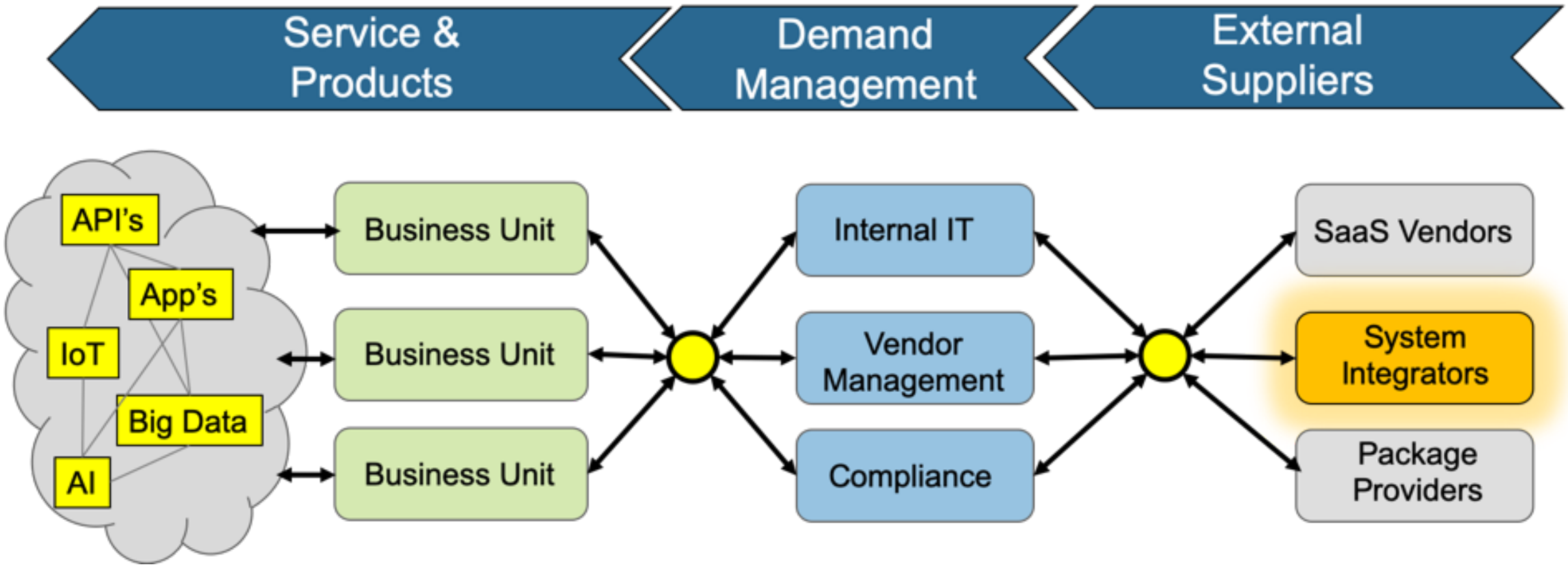


One or Two Poor API's Could Push You Over The Edge

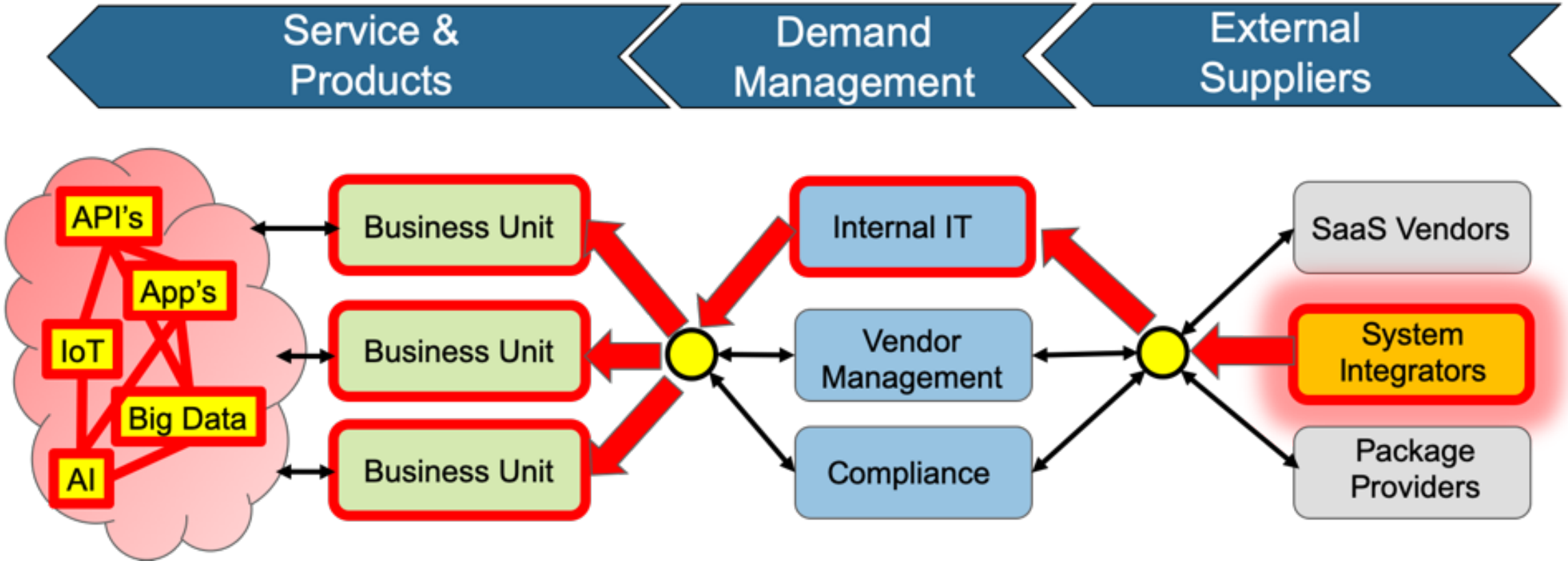
In a nonlinear system, 90% of the complexity is a result of less than 10% of the node connections.

CISQ
Consortium for Information & Software Quality™

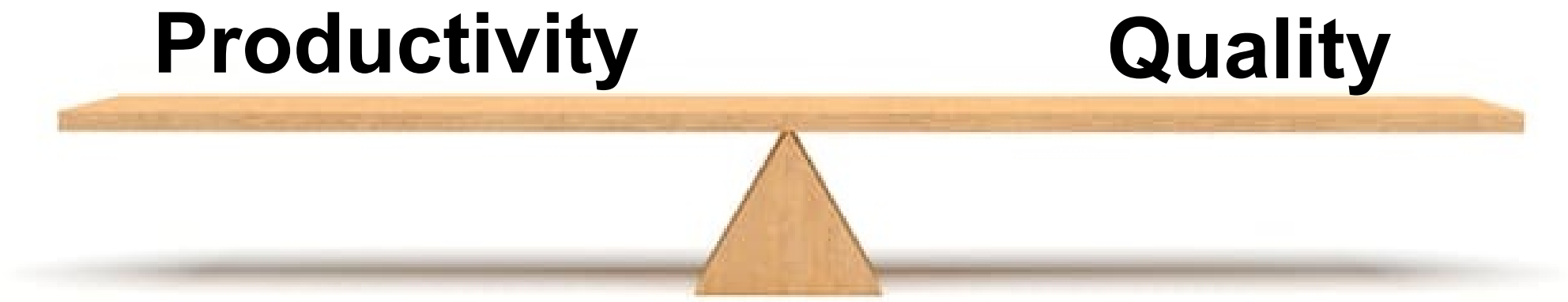
Suppliers Have To Build Quality In From The Start



Suppliers Have To Build Quality In From The Start



Finding The Right Balance Is Difficult, However We Can Make It Easer



We Need Standards We Can Implement With DevOps

We built this city, we built this city on rock an' roll

We Need Standards We Can Implement With DevOps

We built this city, we

On , ISO, CISQ, NIST, etc

k an' roll

CISQ
Consortium for Information & Software Quality™

Let’s Learn From The Past

As industries mature they automate, from robots to fly-by-wire

We Need To Start With Standards

SOFTWARE SIZING	CODE QUALITY	TECHNICAL DEBT
Automated Function Points: Measures the functional size of software	Security: Measures weaknesses in source code representing the most exploited security weaknesses in software including the CWE/Sans Institute Top 25 Most Dangerous Security Errors and OWASP Top 10	Technical Debt: A measure of corrective maintenance effort due to the CISQ code quality weaknesses remaining in a software application
Automated Enhancement Points: Measures changes in the size of both functional and non-functional code during a release in one measure	Reliability: Measures weaknesses in source code impacting the availability, fault tolerance, and recoverability of software	
	Performance Efficiency: Measures weaknesses in source code impacting response time and utilization of processor, memory, and other resources	
	Maintainability: Measures weaknesses in source code impacting the comprehensibility, changeability, testability, and scalability of software	

CISQ
Consortium for Information & Software Quality™

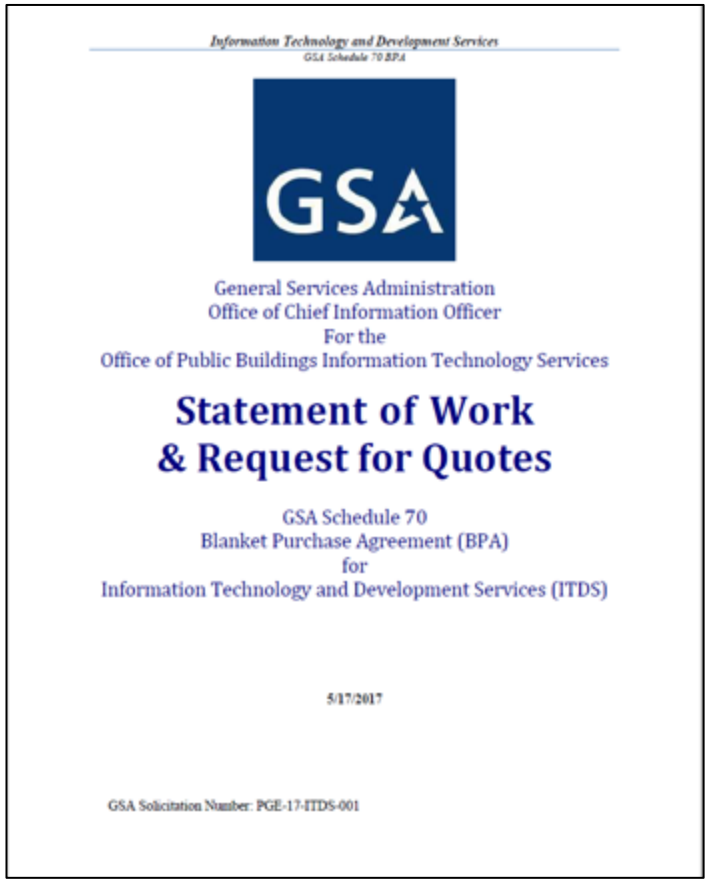
https://www.it-cisq.org/standards/

Building A Trust Relationship Based On Standards

Embed Software Quality & Sizing Standards Into Request For Proposal or Quotes

Embed Software Quality & Sizing Standards Into Request For Proposal or Quotes

Sample RFP



Information Technology and Development Services
GSA Schedule 70 BPA

GSA

General Services Administration
Office of Chief Information Officer
For the
Office of Public Buildings Information Technology Services

Statement of Work & Request for Quotes

GSA Schedule 70
Blanket Purchase Agreement (BPA)
for
Information Technology and Development Services (ITDS)

5/17/2017

GSA Solicitation Number: PGE-17-ITDS-001

CISQ has been referenced by the U.S. General Services Administration (GSA), **formally citing CISQ requirements in a Information Technology (IT) statement of work from the Office of the CIO for the Office of Public Buildings**. GSA is an independent agency of the U.S. government that supports general services of Federal agencies.

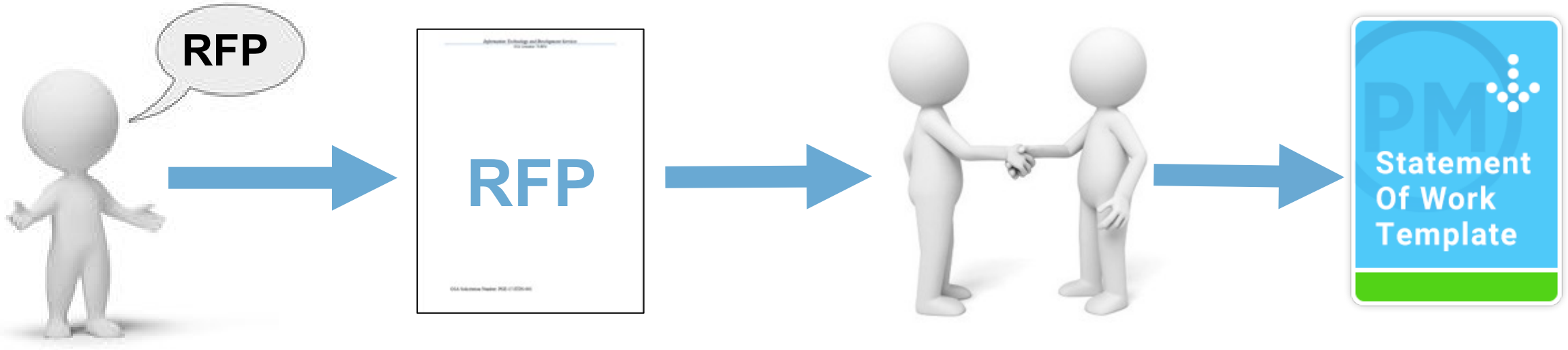
See page 21, section 5.9 in GSA's document, Schedule 70 Blank Purchase Agreement for IT and Development Services…

"PB-ITS (Project Based IT Services) is seeking to establish code quality standards for its existing code base, as well as new development tasks. As an emerging standard, PB-ITS references the ***Consortium for Information Software Quality (CISQ) for guidance on how to measure, evaluate and improve software****."*

CISQ
Consortium for Information & Software Quality™

Agree Productivity Levels With Suppliers Based On Automated Sizing Code – Combine With Manual Sizing Of Requirement

Embed The Agreed Sizing Method and Productivity Into The Statements of Work



Embed The Agreed Sizing Method and Productivity Into The Statements of Work

1. **Contracting and Productivity**

1. **Productivity**

   The contracted is based on a bases level of productivity of **18 Function Pointers per Staff Month** [1]. A staff month is defined as 22 days per calendar month, 8 hours per day, equalling 176 working hours per month.

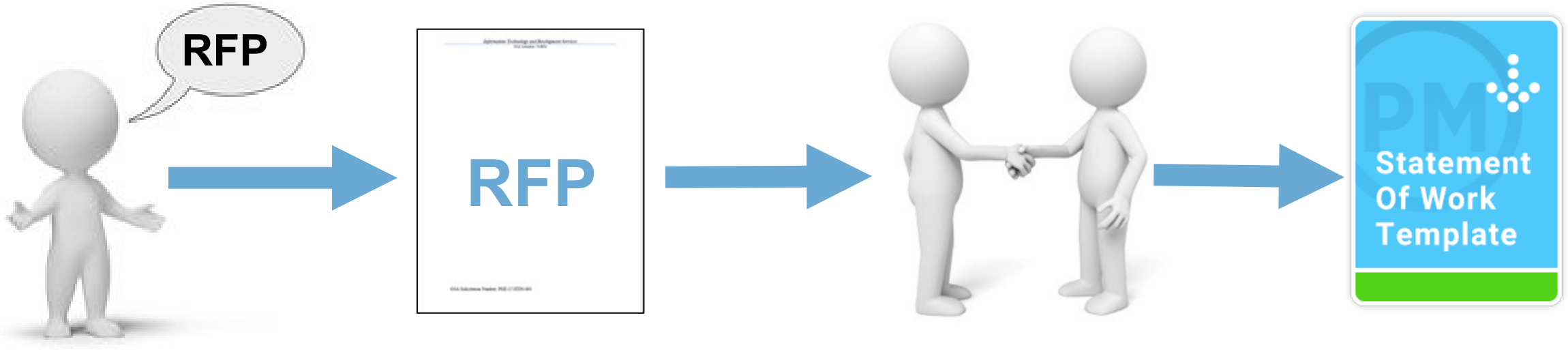
   Attentively the contracted is based on a bases level of productivity of 9.5 hours per function point [1].

1. **Rate**

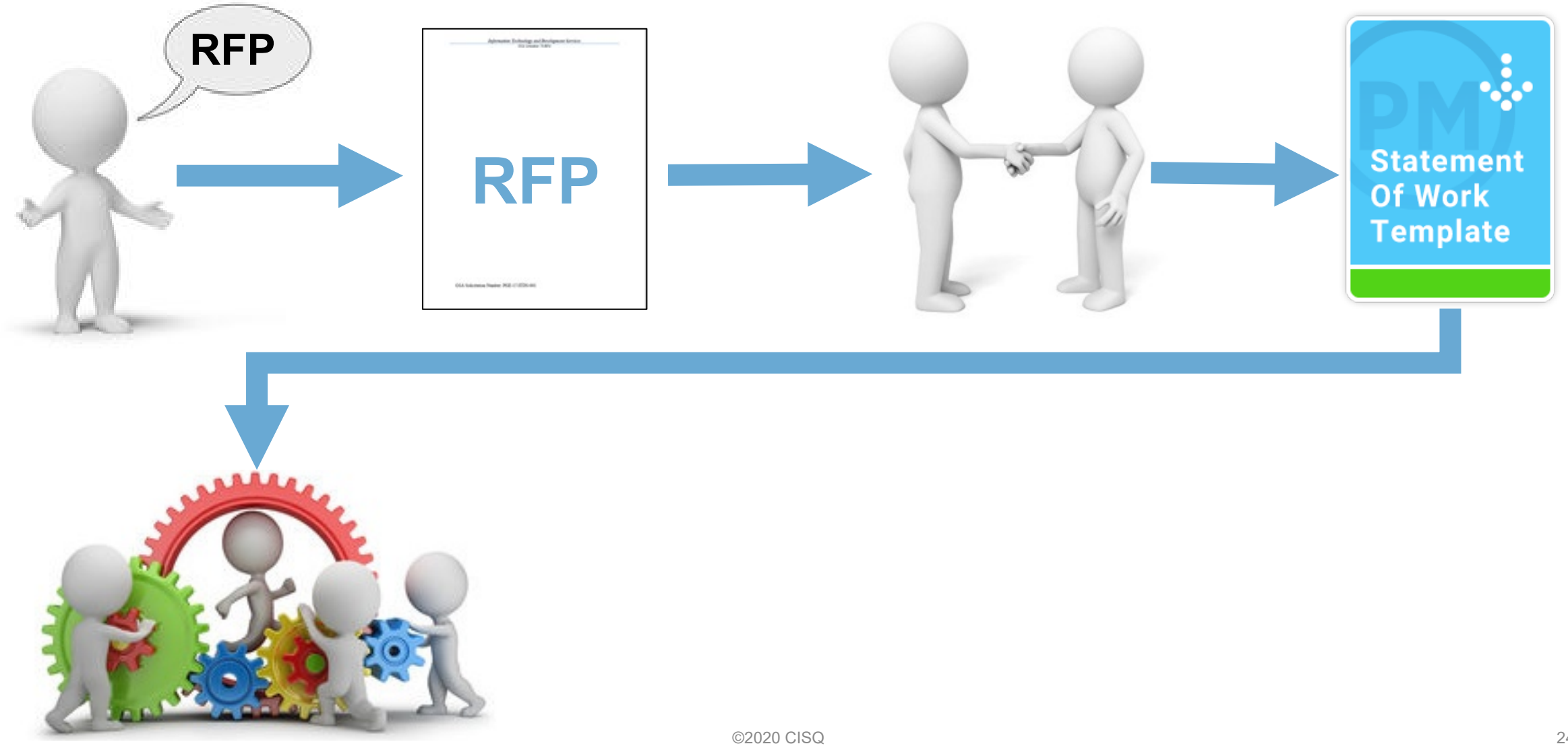
   The supplier shall invoice at a rate of € 300 [2] per function point delivered to the client as measured by **ISO 19515 Information technology — Object Management Group Automated Function Points (AFP), 1.0** defined in section 3.4

   Exceptions to the rate and activities that will not be invoiced by function point must be agreed in advance of contract signing.

Suppliers Should Be Ready To Develop to the Standards



Suppliers Should Be Ready To Develop to the Standards



Suppliers' Teams Should Use Tools That Support CISQ AFP and ISO Sizing Standards

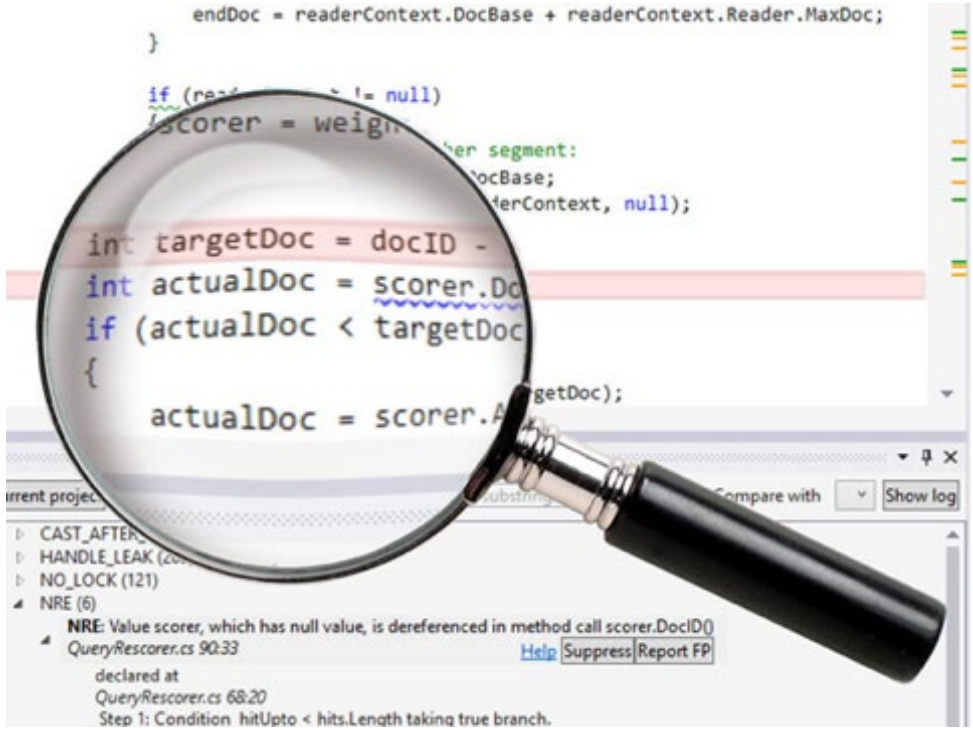
avaJava.com Web Tutorials - Eclipse

TestServlet.java

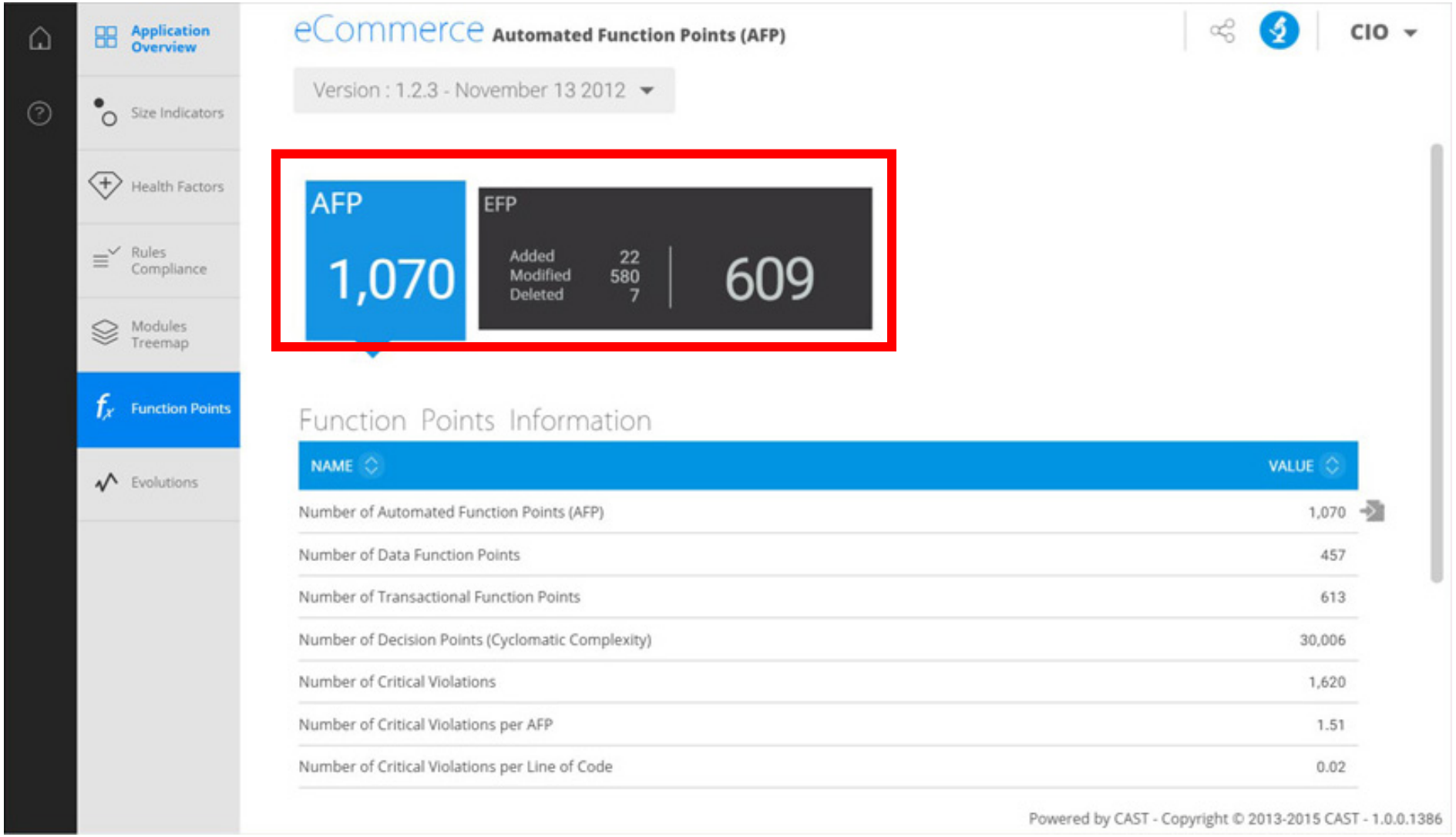
```java
package my;

import java.io.IOException;

import javax.servlet.Servlet;
import javax.servlet.ServletException;
import javax.servlet.http.HttpServlet;
import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletResponse;

public class TestServlet extends HttpServlet implements Servlet {
    static final long serialVersionUID = 1L;

    public TestServlet() {
        super();
    }

    protected void doGet(HttpServletRequest request,
            HttpServletResponse response) throws ServletException, IOException {
        doPost(request, response);
    }

    protected void doPost(HttpServletRequest request,
            HttpServletResponse response) throws ServletException, IOException {
        response.getWriter().println("blah");
    }
}
```

How do I create a profile to format Java code in Eclipse?

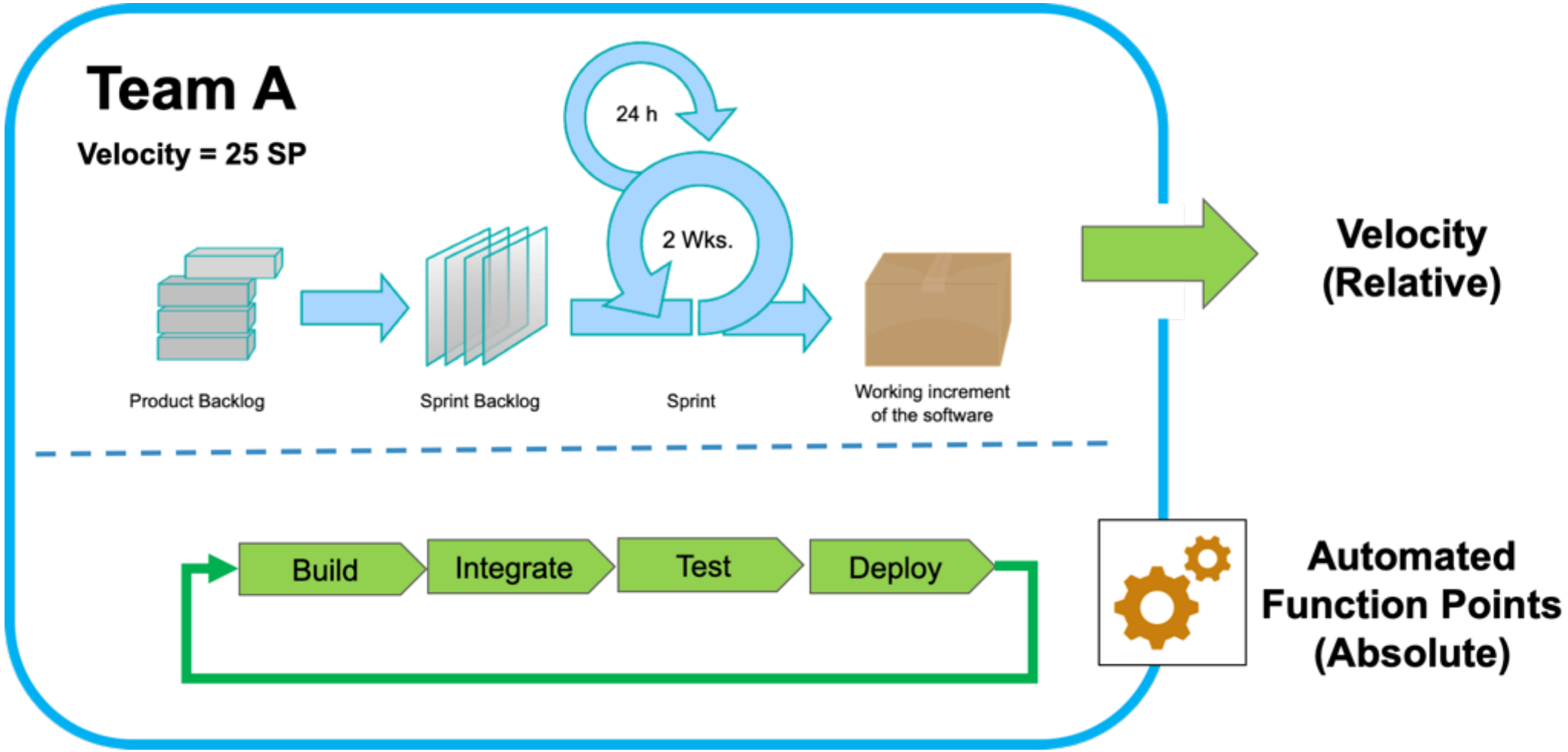
Automatic Analysis Of The Size Of The Code In Function Points



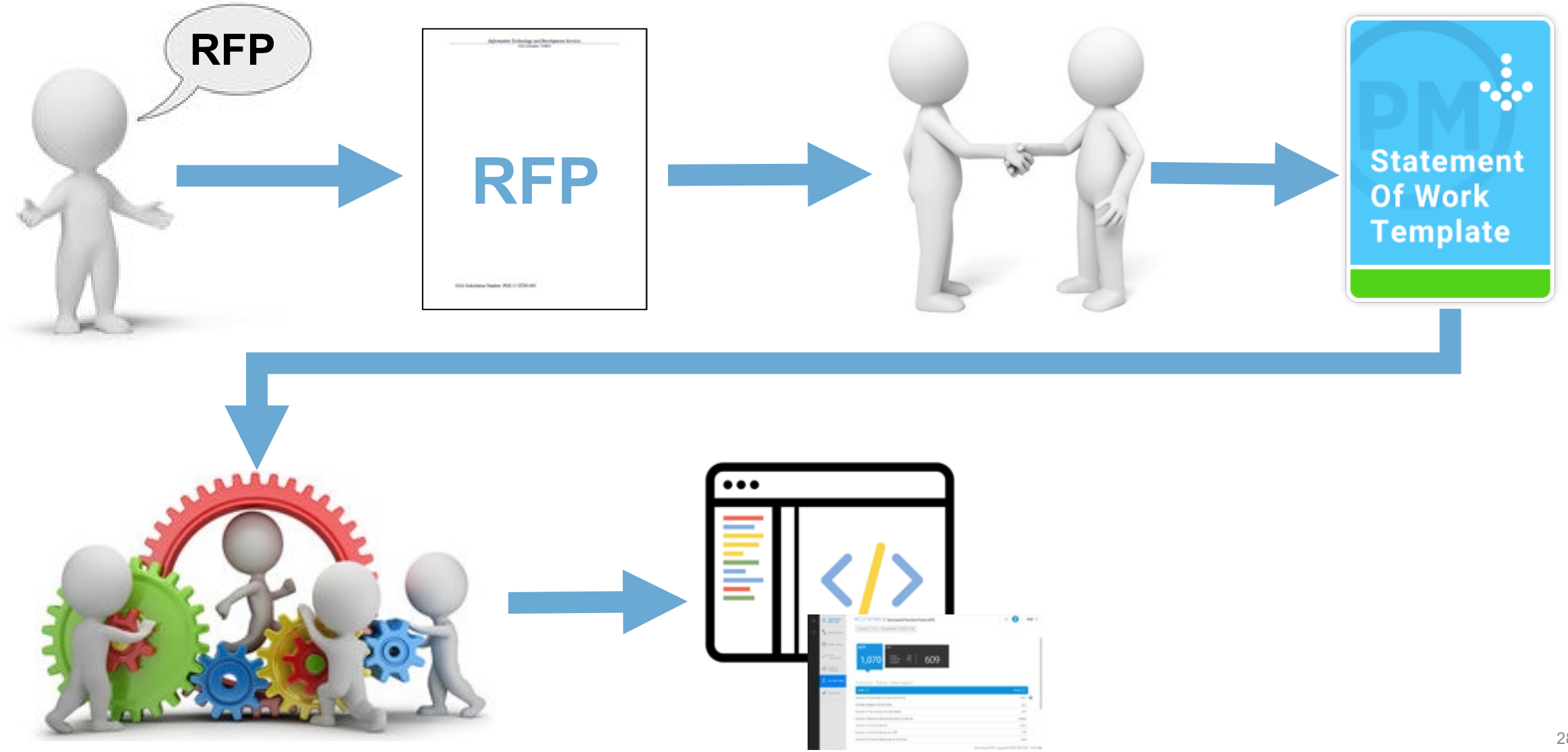
Team Dashboards Should Clearly Show The Size Of Code Developed and Enhanced



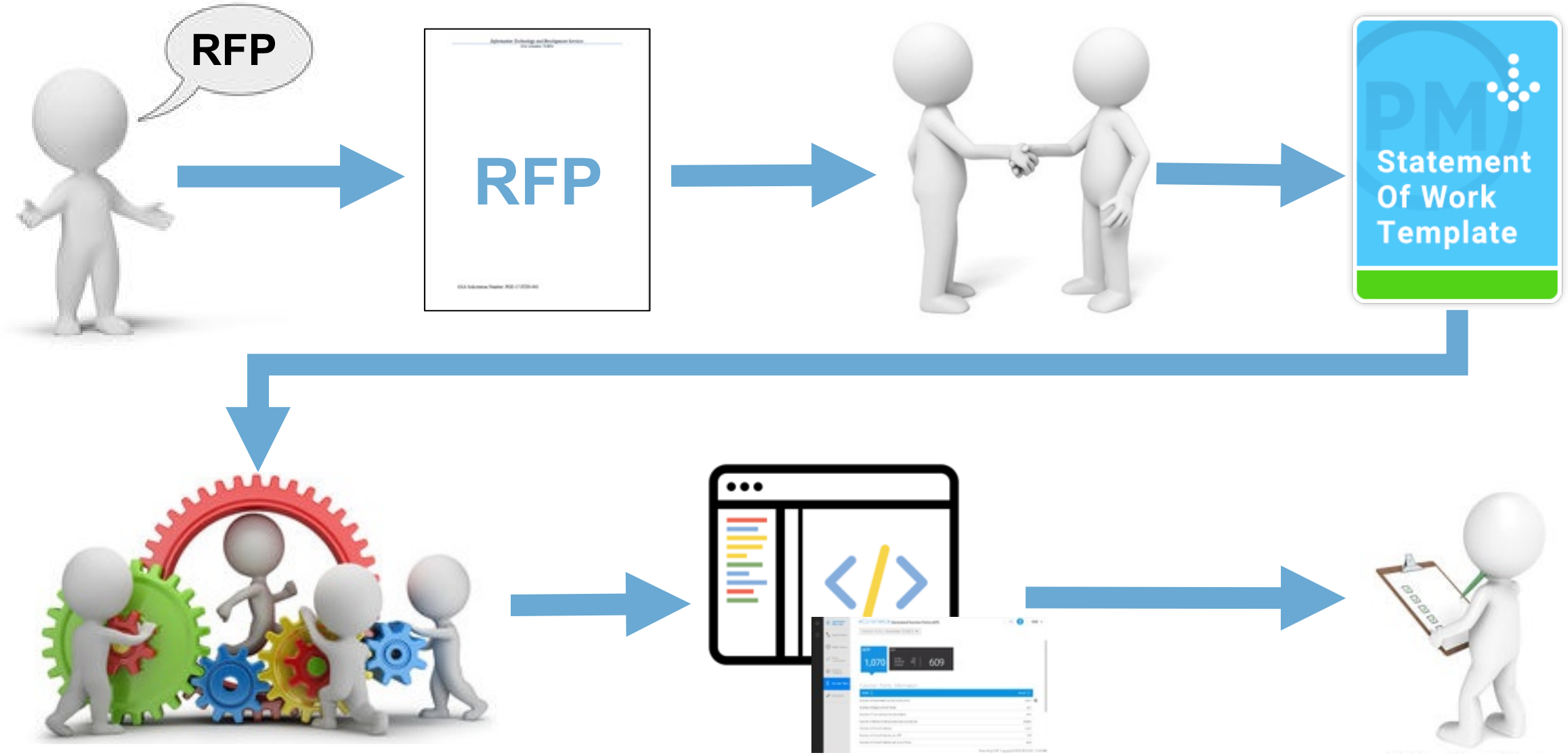
Teams Are Still Free To Use Agile & DevOps Story Point Sizing, Automated Function Points Counted In The Background



Do Not Just Focus On Size of The Code, Verify The Quality – Automatically

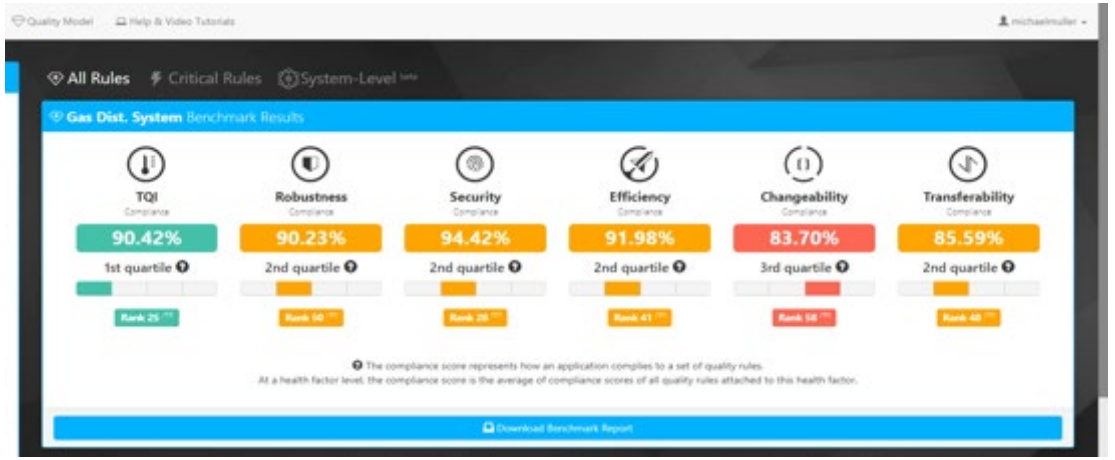


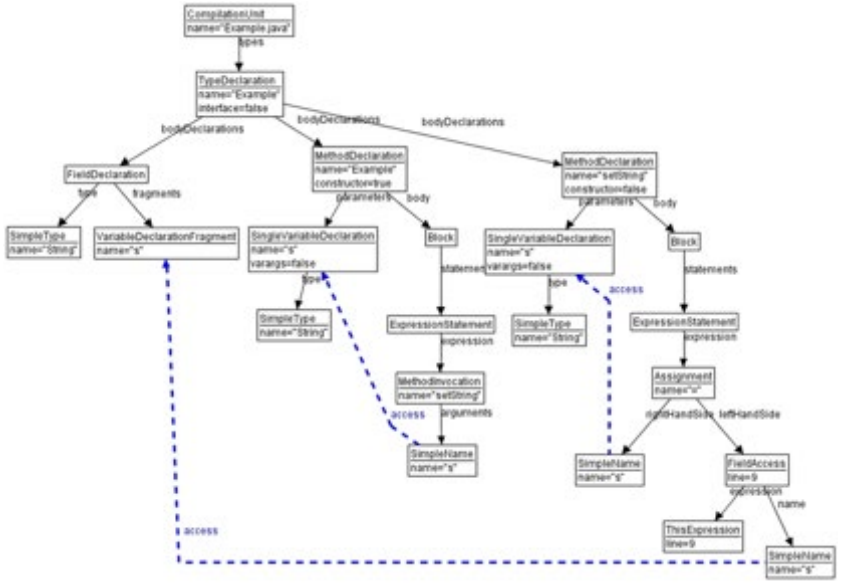
Do Not Just Focus On Size of The Code, Verify The Quality – Automatically



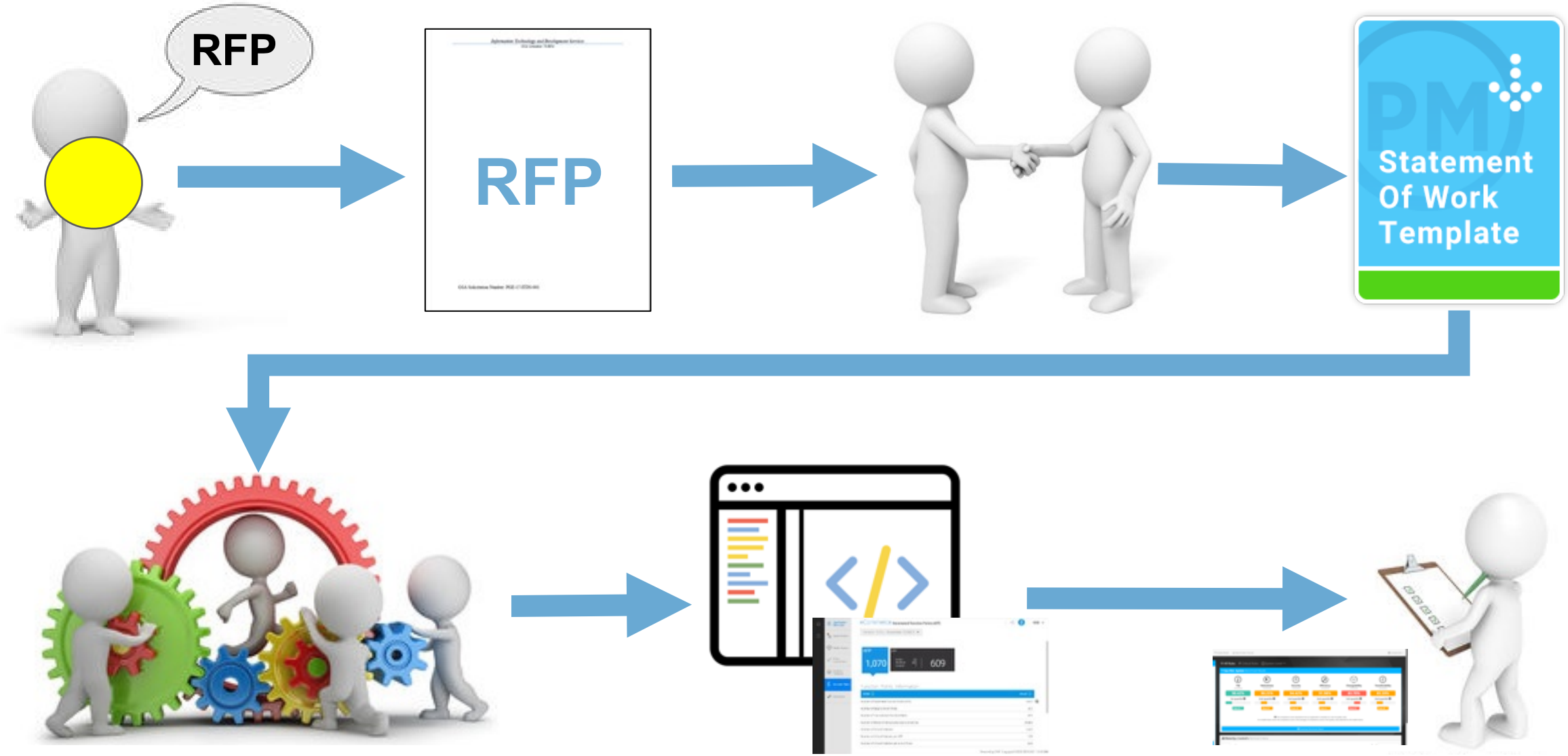
Suppliers Teams Should Verify Code Quality, and Check For Vulnerabilities Against CISQ Standards

- Security: Measures weaknesses in source code representing the most exploited security weaknesses in software including the CWE/Sans Institute Top 25 Most Dangerous Security Errors and OWASP Top 10
- Reliability: Measures weaknesses in source code impacting the availability, fault tolerance, and recoverability of software
- Performance Efficiency: Measures weaknesses in source code impacting response time and utilization of processor, memory, and other resources
- Maintainability: Measures weaknesses in source code impacting the comprehensibility, changeability, testability, and scalability of software
- Technical Debt: A measure of corrective maintenance effort due to the CISQ code quality weaknesses remaining in a software application





End to End Trust Relationship Based On Standards



Building A Foundation Quality Standards That Fit Modern Methods and Architecture

Quality Standards That Are :

- Automated
- Product focused vs project
- Support Event and API Architecture
- Integrated in to DevOps & DevSecOps Toolchain

CISQ
Consortium for Information & Software Quality™

Focus on Culture and Behavior – Be Specific

- **Don’t expect everyone to like automation, some people just like doing it the hard way**
- **Incentivize the behavior you want for the individual and team.**
- **Have agreed metrics and KPI linked to automation.**
- **Show results**

CISQ
Consortium for Information & Software Quality™

Develop The Correct Skills, But Focus More on Behaviors

Standards Champion (A Hard Role)

Engineering Value Stream Design

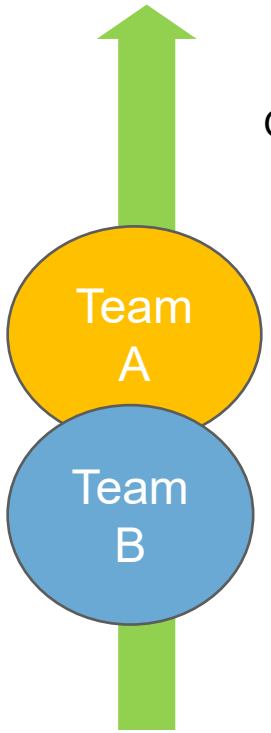
Dashboard Design

Toolchain Integration

Stay in Control With Agile Governance – Don't Push From The Top, Grow From The Bottom

- **Communities of Practice**
- **Lease Train Toolchain Consistency**
- **Automation Best Practice**

Gamify - Link Automation & Consistency to Team Autonomy



Freeze Periods

Only exceptional change freeze periods apply

All freeze periods apply

Change Advisory Board

CAB for information purposes only

CAB for all changes

Frequency of Deployments

No limits on changes per today

Few changes per week

Time of Deployments

Intra-day allowed

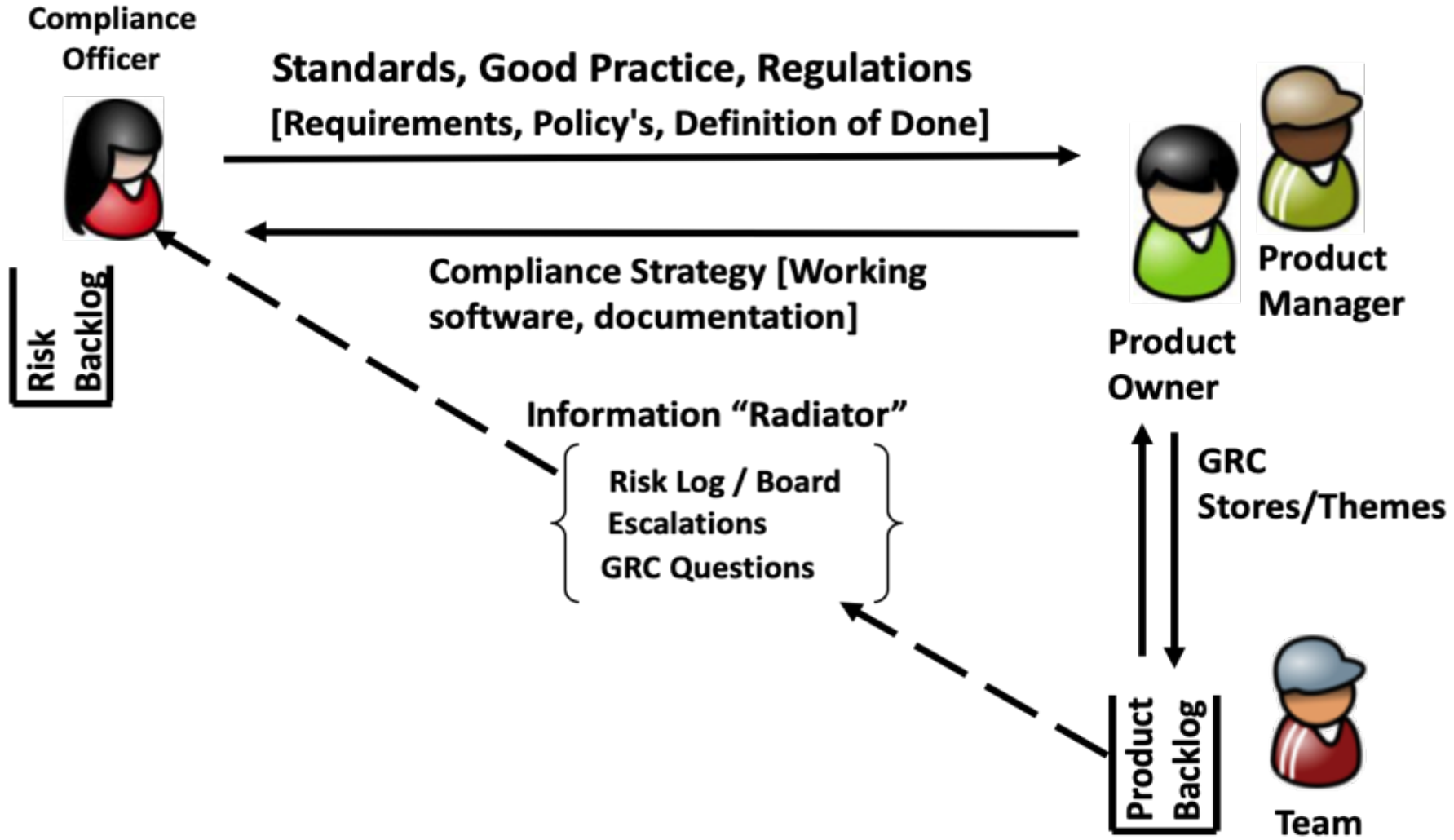
After hours and on weekends

Level of Automation

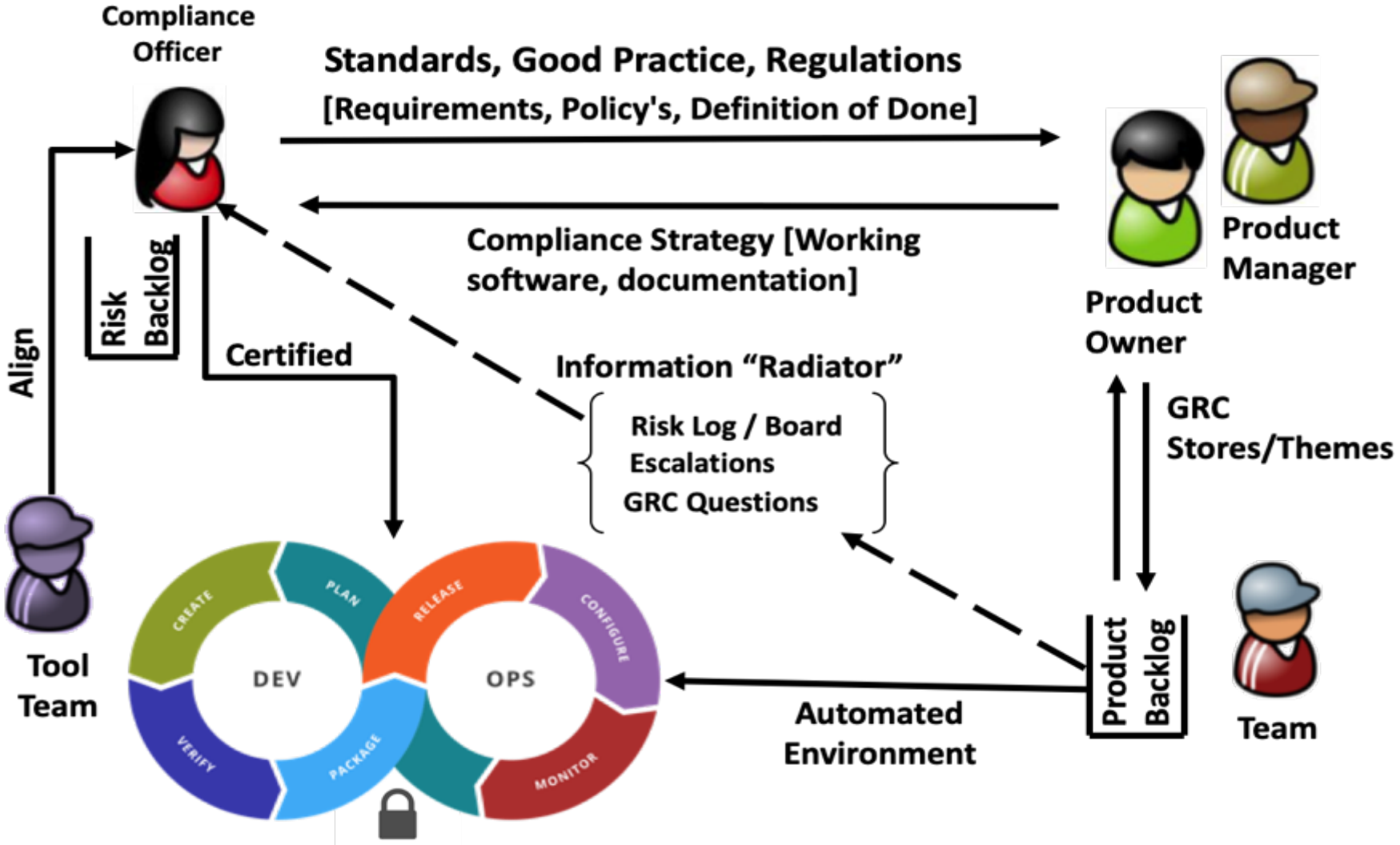
Continuous Integration	Quality Assurance	Coding Practices
Release Management	Incident Management	Environments

CISQ
Consortium for Information & Software Quality™

Obtain Commitment From The Team and Product Owner Agreement



Certify The Environment and Lock It Down, But Make Sure There Is A Process To Change It Quickly and Consistetly



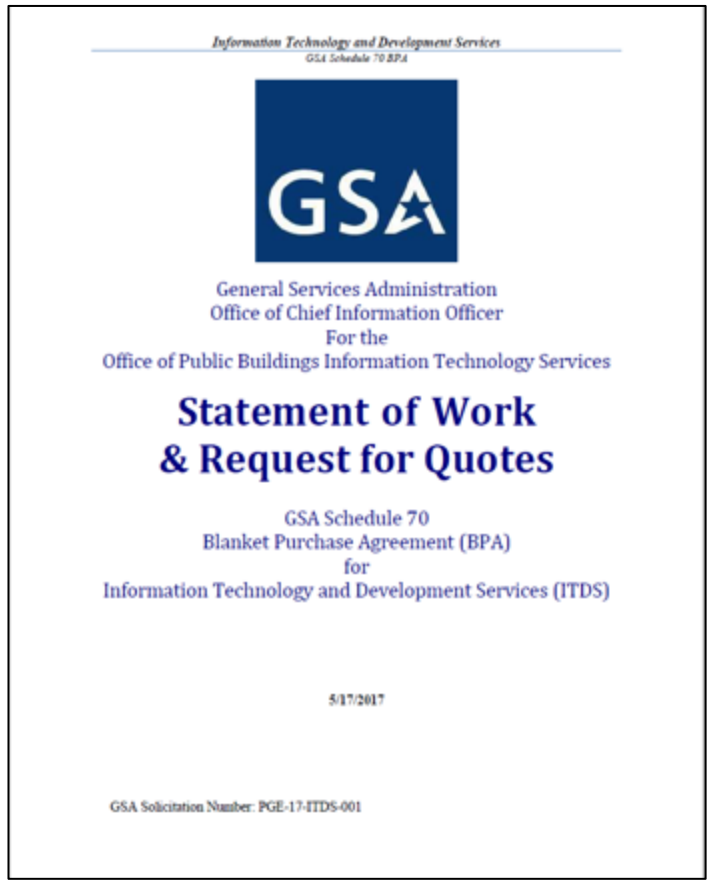
Set Targets Based On CISQ Measures To Reduce TCO

- **Security**: Security weakness and vulnerabilities
- **Reliability**: Availability, fault tolerance, and recoverability of software
- **Performance Efficiency**: Response time and resources utilization
- **Maintainability**: Changeability, testability, and scalability of software
- **Technical Debt**: Corrective maintenance effort

CISQ
Consortium for Information & Software Quality™

Build Standards Into The Contract

Sample RFP



Information Technology and Development Services
GSA Schedule 70 BPA

GSA

General Services Administration
Office of Chief Information Officer
For the
Office of Public Buildings Information Technology Services

Statement of Work & Request for Quotes

GSA Schedule 70
Blanket Purchase Agreement (BPA)
for
Information Technology and Development Services (ITDS)

5/17/2017

GSA Solicitation Number: PGE-17-ITDS-001

CISQ has been referenced by the U.S. General Services Administration (GSA), formally citing CISQ requirements in a Information Technology (IT) statement of work from the Office of the CIO for the Office of Public Buildings. GSA is an independent agency of the U.S. government that supports general services of Federal agencies.

See page 21, section 5.9 in GSA's document, Schedule 70 Blank Purchase Agreement for IT and Development Services…

"PB-ITS (Project Based IT Services) is seeking to establish code quality standards for its existing code base, as well as new development tasks. As an emerging standard, PB-ITS references the Consortium for Information Software Quality (CISQ) for guidance on how to measure, evaluate and improve software."

CISQ
Consortium for Information & Software Quality™

Working With Suppliers & CISQ

Six Levels of Engaging Vendors with CISQ Standards

Recommendation email

- ✓ Email to vendor delivery leaders that they should consider using CISQ guidelines for all ADM work

RFP

- ✓ Initial statement of requirements and project definition can set the tone for quality of deliverables

SLAs

- ✓ Treat software enhancements and maintenance as a service; track levels, penalties, credits

SOW

- ✓ Definition of specific project scope and deliverable can include definition of quality and security

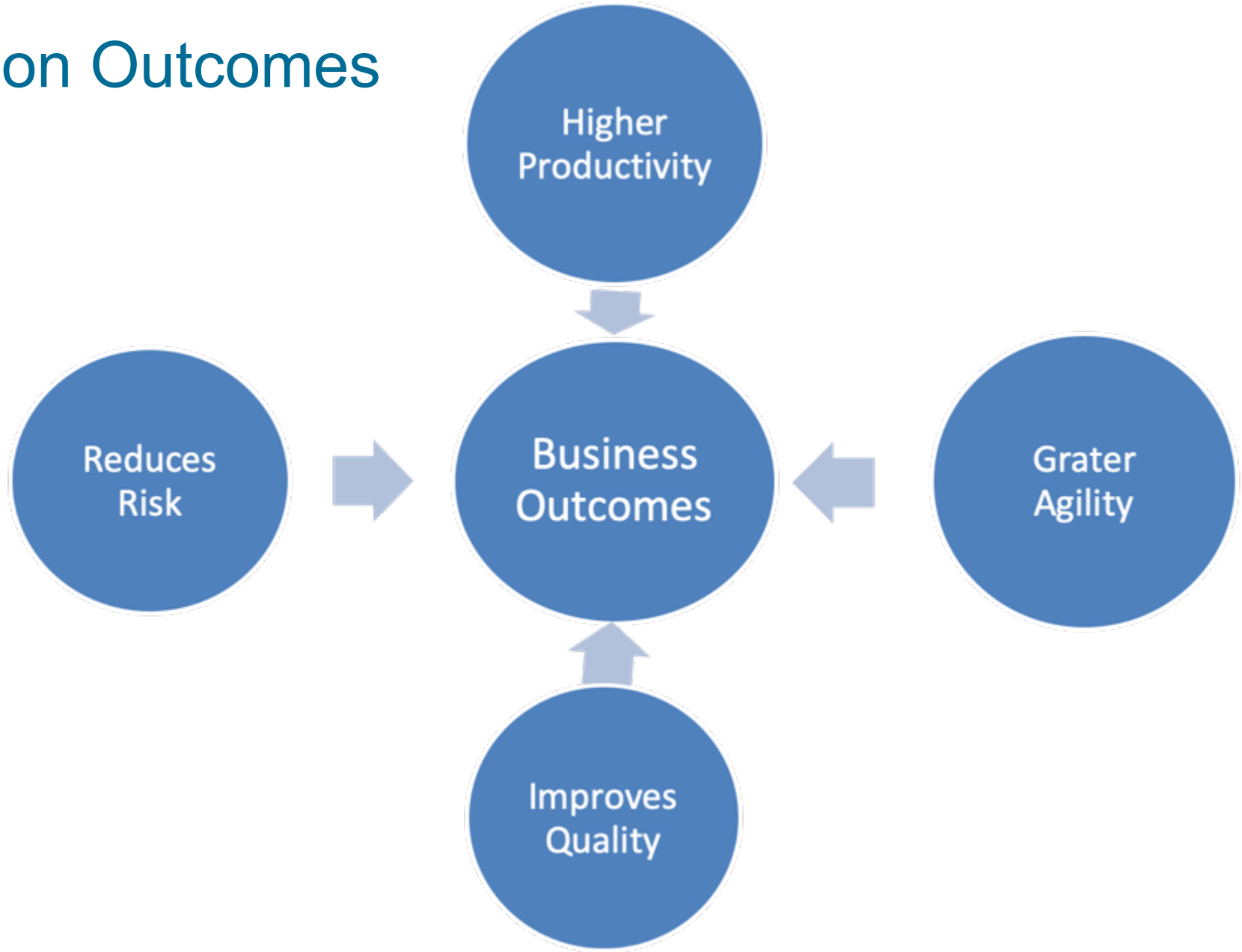
Scorecard

- ✓ Measurement and discussion in governance committees to help set behavior

Acceptance criteria

- ✓ Measure and demand minimal set of acceptance criteria for any new development or release

Focus on Outcomes



Use CISQ Guidelines To Help You On Your Journey

- Using Software Measurement in SLAs: Integrating CISQ Size and Structural Quality Measures into Contractual Relationships
- Sample Acceptance Criteria with CISQ Standardized Metrics
- Contracting Best Practice - Improve Supplier Productivity Using the Automated Function Point Standard
- Contracting Best Practice - Lower Risk and Improve Outcomes with Suppliers by Using Software Structural Quality Standards

Help Us Develop The Next Generation Of Digital Standards

JOIN THE INDUSTRY-LEADING CONSORTIUM ADVANCING SOFTWARE QUALITY MEASUREMENT

The Consortium for Information & Software Quality™ (CISQ™) puts Information Technology (IT) leaders in the position to directly participate in the development of industry standards and methodologies for measuring the quality and trustworthiness of software. Members include IT executives and practitioners in charge of significant mission-critical applications from many enterprises, systems integrators and public sector institutions across the globe.

INDIVIDUAL MEMBERSHIP

Would you like to stay updated on this work and network with members in the community? Individual membership is free.

- Subscribe to CISQ's email list
- Receive updates on the standards
- Receive technical guidance documents
- Receive event invitations

JOIN NOW

CORPORATE MEMBERSHIP

Would you like to contribute to the standards and participate in deployment activities? Your organization is invited to become a corporate member and sponsor the work that CISQ undertakes. Sponsorship is open to companies, government agencies, not-for-profit, and academic institutions.

- Team members participate in working groups
- An executive joins the Governing Board
- Your organization is listed as a supporter of all CISQ events, including complimentary passes and an exhibit table
- See benefits of corporate membership

JOIN NOW | I'M INTERESTED IN SPONSORSHIP

CISQ
Consortium for Information & Software Quality™