

Empowerment Quality Engineering

Thinking Risk to Determine Strategy

Barry McManus

Quick Question...

days a hack goes undetected/contained is?

10

50

146

175

206

250

279

365+

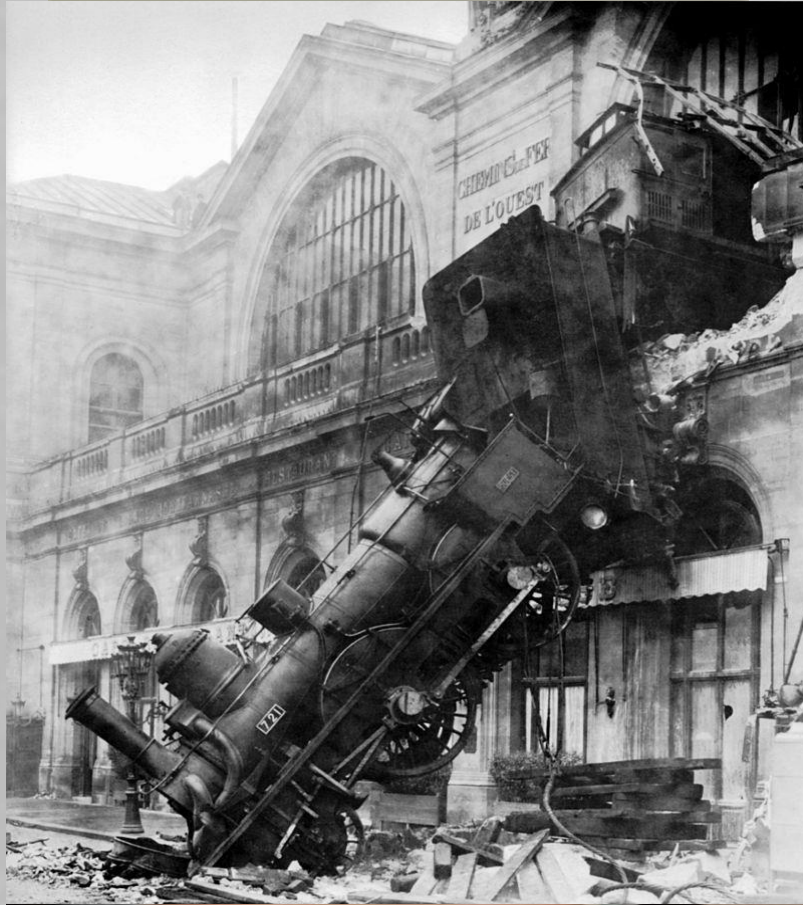
Empowerment Quality Engineering

- ▶ Computerised Systems Value Consultancy:
 - ▶ Technical stuff!
 - ▶ Quality stuff!
 - ▶ Bridge between IT & Quality

Disclaimer - A large topic discussion in a short period of time.

Disclaimer - These are the views of Empowerment Quality Engineering.

Empowerment Quality Engineering



Defect:

A bug that causes an incorrect result or system failure

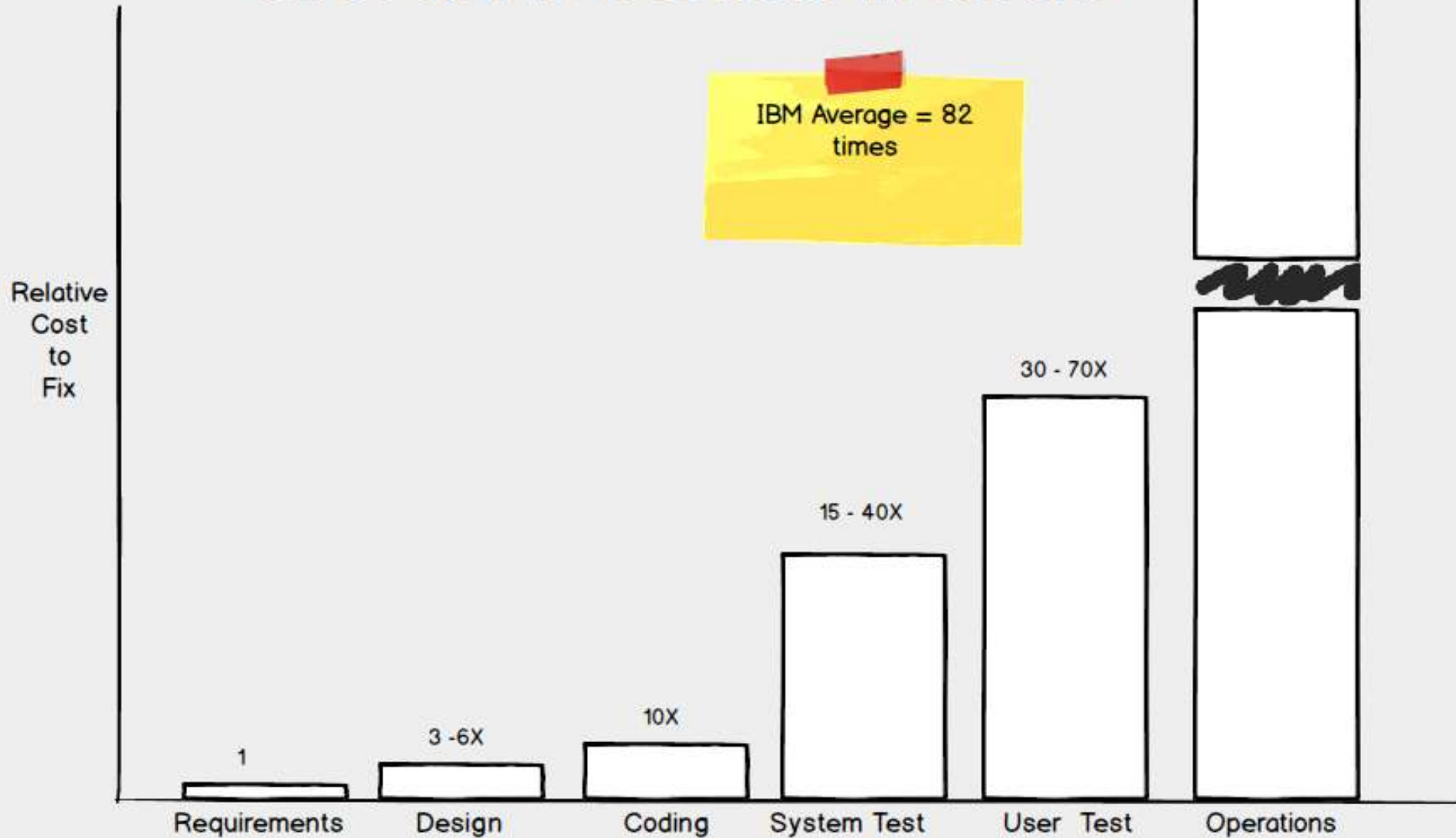
Security Vulnerabilities:

Defects that enable a system to be compromised

Franken-algorithms: the deadly consequences of unpredictable code

The death of a woman hit by a self-driving car highlights an unfolding technological crisis, as code piled on code creates 'a universe no one fully understands'

Cost to Fix Defects in SDLC



Dick Cheney's Heart implant attack was credible

🕒 21 Oct

GDPR FINES

IDENTITY THEFT

Dick Cheney, the former US vice-president, has revealed his heart implant was the result of a terrorist attack.

ESPIONAGE

Mr Cheney's doctor said the heart defibrillator was implanted in 2007 to protect him from assassins from interfering with it and causing a fatal heart attack.

PHYSICAL HARM



REPUTATION

Former US vice-president Dick Cheney has suffered from heart problems for much of his life.

As Easy
As...

Boy, 11, hacks cyber-security audience to give lesson on 'weaponisation' of toys

Reuben Paul, 11, tells conference that smart cars, fridges, lights and even teddy bears can be used to spy on or harm people

“From airplanes to automobiles, from smartphones to smart homes, anything or any toy can be part of the **Internet** of Things (IOT),” said the small figure pacing the huge stage at the World Forum in The Hague.

To demonstrate he deployed his cuddly bear, which connects to the cloud via wifi and Bluetooth to receive and transmit messages.

Plugging into his laptop a device known as a “Raspberry Pi” - a small credit-card size computer - Reuben scanned the hall for available Bluetooth devices, and to everyone’s amazement including his own, suddenly downloaded dozens of numbers, including some of top officials.

Regulatory focus on security

	Annex 11	21 CFR Part 11	OECD 17	Guidance	
Security (Operational focus)	12; 12.1; 12.2; 12.3; 12.4	11.10(c); 11.10(d); 11.10(e); 11.10(g); 11.300	1.9; 2.2; 2.9; 3.6; 3.7	PIC/S 011_03 6.2; PIC/S 041_01 9.3; ICH e6 4.1.5; 5.5.3 (c); (d); (e); GDPR 5.1 (f). 32. ISO-27001	
Security (Building into software)			-	MHRA GMP PIC/S 010_01 10.2 IEE OWASP	IT spend increasing: \$101bn: 2017 \$114bn: 2018 \$124 Billion: 2019 (Gartner)
	Good SOP Focus: Backup; Retrieval; Encryption; Pen Test; Monitoring...				2018 6.20

Cost of a data breach highlights

Global Averages



Average size of a data breach

25,575 records

Average total cost of a data breach

\$3.92M

Cost per lost record

\$150

Time to identify and contain a breach

279 days

Highest country average cost of \$8.19 million

United States

Highest industry average cost of \$6.45 million

Healthcare

The soft “underbelly” of Computerised Systems

Over 92% of reported vulnerabilities exist in software and not in networks (Security Week).

- ▶ 75% of security breaches occur at the software layer (Gartner).

Outer network defenses are “cracked” to access the “soft” inner code to:

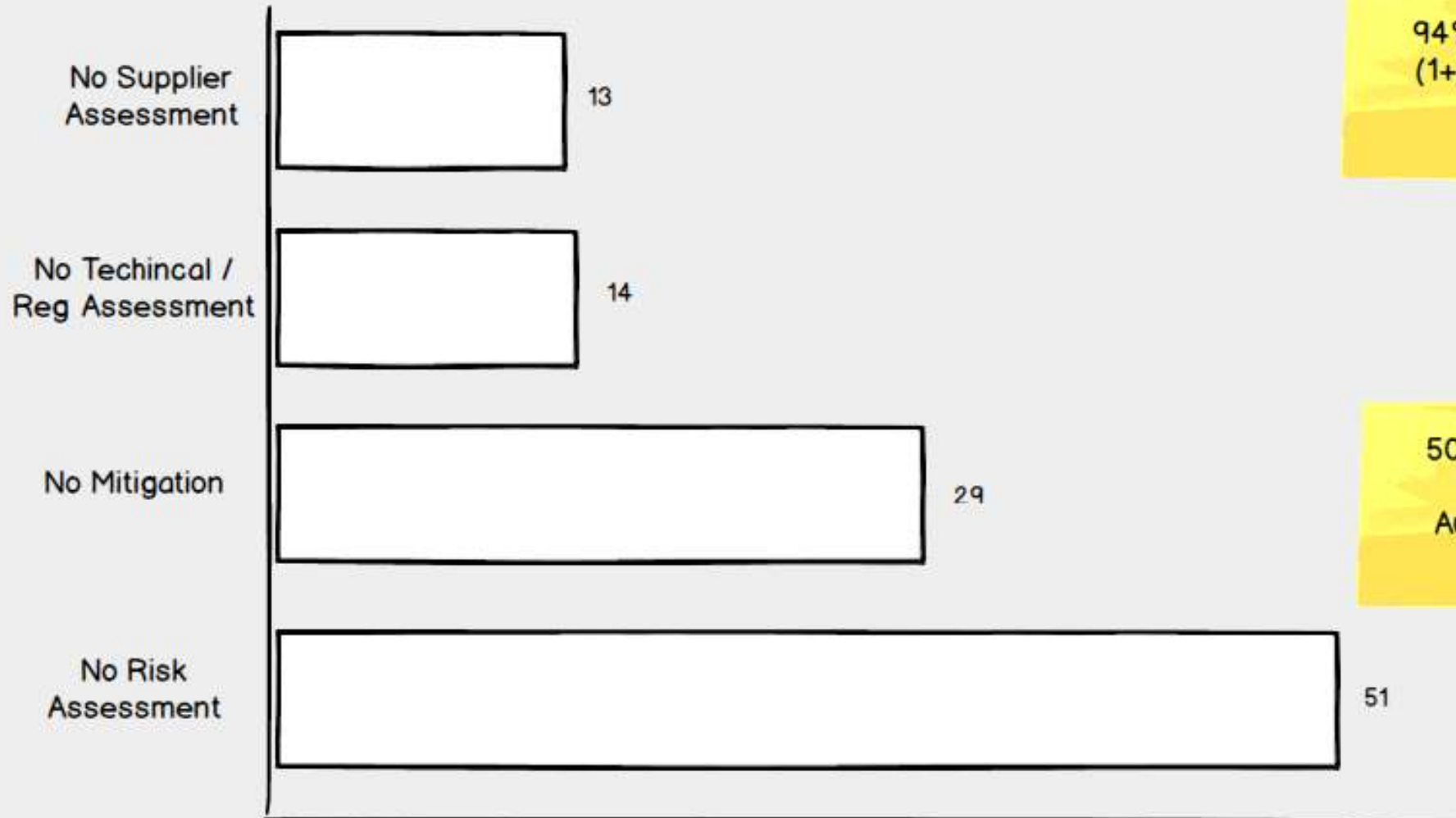
- ▶ Falsification: to change Clinical Trial Data.
- ▶ Falsification: Switch off Audit Trail.
- ▶ Ransom: Deny access to records.
- ▶ Identity Theft: PII - birth certs; credit card; social security number (\$1 dark web).

Talk about Risk... again!

Need RISK to focus our Economics, Our Time, **OUR QUALITY!**

- ▶ Focus our time to prevent issues (GDPR “design security in”).
- ▶ Focus our time to identify issues earlier (Patient health).
- ▶ Why spend time on something that is not important?

Risk Deficiency: Audit Findings - 50 Audits



94% of Audits = (1+) risk finding!

50 Compliance & Supplier Audits - ('17-'18)

5 Stage Risk Process

	Stage	Activity
1	Analyse	Requirements Elicitation & Review
2	Creative	Identify & Quantify Your Risks
3	Evaluate	Identify Mitigations for each Risk
4	Measure	Assess the effectiveness of each Mitigation
5	Repeat	Re-assess (Manage) at key stages

Risk Stage: 1 - Analyse

Transfer data from isolated “PC A” to isolated “PC B”.

Req ID ▲	UR-TFR-001 ◆	Version #	1.0a
Title:	Transfer data from isolated “PC A” to isolated “PC B”		
Goal:	“PC A” Data is available on “PC B”		
Rationale:	Required for processing as per SOP 1234 v2.1		
Type:	Functional Process Regulatory		
Priority:	Must Have		
Owner:	Barry McManus		
Risk:	High		

Risk Stage: 2 - Creative

- Checklists

- Comparison with past experiences.

- Tools e.g. Walk backward (Ishikawa diagrams):

- What is the potential failure?
- Work backwards from that failure.
- What scenarios arise leading to the failure?
- What risks could have created the scenario?

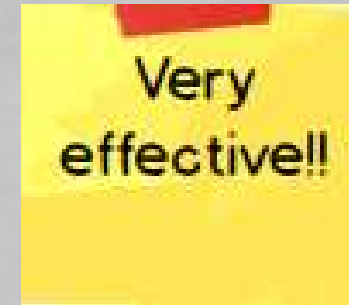
Creative & Critical Thinking:

- Patient Safety, Data Integrity, Quality!

Risk Stage: 2 - Creative (Critical)

How to think Critically & Creatively:

- Warm up exercise
- Brain writing (individual perspective)
- General brain storming - Anything goes!
- Use checklists to stimulate creativity
- **No Criticism (of people)!**



Risk Stage: 2 - Creative

Simplest Approach:

Rudyard Kipling's 5W's (+)

I KEEP six honest serving men
(They taught me all I knew);

Their names are **What** and **Why** and **When**
And **How** and **Where** and **Who**.



Risk Stage -2 - Creative - 5 W's

Req ID ▲	UR-TFR-001 ◆	Version #	1.0a
Title:	Transfer data from isolated "PC A" to isolated "PC B"		

What: Data is compromised.

Why: "Manually Transfer data between 2 isolated PCs".

Who: Data transfer role.

Where: on PC A, on transfer media, on PC B.

When: Transfer from PC A to transfer media.

How: Human interference.

How: Transfer media fatigue.

An Initial risk assessment may look like...

Risk Stage -2- Creative (Risk Identification)

Req-ID	Req-Description	Risk-ID	Risk-Description	Your Risk Calculation
UR-TFR-001	Manually Transfer data between 2 isolated PCs	R-001.1	Data Transfer is compromised by - direct changes by operator corruption	High
		R-001.2	Data Transfer is compromised by - data corruption from transfer media	High

Risk Stage -3- Evaluation

What should be done about the risk(s)...?

- ▶ **Avoid** (use known technology)
- ▶ **Absorb** (deal with the consequences)
- ▶ **Reduce** (seek to reduce)
- ▶ **Monitor** (regularly review the risk probability/impact)
- ▶ **Refuse** (refuse to accept the risk from your supplier)

Low risk items receive less focus than high risk items!

Risk Stage: 3 - Evaluation - Reduce/Mitigate

- ▶ What could potentially be done to reduce the risk materialising in the production environment?
 - ▶ Technical controls?
 - ▶ Manual controls?

Risk Stage: 3 - Evaluation - Mitigate

Req-Description	Risk-ID	Risk-Description	Your Risk Calculation	Mitigation-ID	Mitigation-Description
Manually Transfer data between 2 isolated PCs	R-001.1	Data Transfer is compromised by - direct changes by operator corruption	High	M-R-001.1-1	Automate data transfer onto transfer media
				M-R-001.1-2	Encrypt the transfer media storage to prevent access during transit.
				M-R-001.1-3	Create audit trail logs at: - data copy (source) onto transfer media - data copy (target) from transfer media - data copy/read (unapproved target) from copy media (audit trail stored with data transfer)
	R-001.2	Data Transfer is compromised by - data corruption from transfer media	High	M-R-001.2-1	Add a Cyclic Redundancy Check (CRC) of the data record to indicate corruption during transit.
				M-R-001.2-2	Retain data copy at origin until target confirms correct transfer
	R-001.3	Operator unaware of operation failures: e.g. failed backup failed data transfer failed encryption	Medium	M-R-001.3-1	Implement operation return codes for (in)correct processing. Aid ease of : - understanding - maintenance

Risk Stage: 4 - Measure - Quality Activities

Mitigation-ID	Mitigation-Description	Design-ID	Design Description	Design Review
M-R-001.1-1	Automate data transfer onto transfer media	D-001.1-1	UML Describe automatic transfer of data onto medium: Use Case - Data design - Process Flow - State Transition Chart	<Enter Date>
M-R-001.1-2	Encrypt the transfer media storage to prevent access during transit.			
M-R-001.1-3	Create audit trail logs at: - data copy (source) onto transfer media - data copy (target) from transfer media - data copy/read (unapproved target) from copy media (audit trail stored with data transfer)			
M-R-001.2-1	Add a Cyclic Redundancy Check (CRC) of the data record to indicate corruption during transit.			
M-R-001.2-2	Retain data copy at origin until target confirms correct transfer			
M-R-001.3-1	Implement operation return codes for (in)correct processing. Aid ease of : - understanding - maintenance			

Design-Review = Quality Gate

Feedback for Supplier & You:

Indication of:

- progress issues?
- technical complexity?
- data control flow?
- error handling & recovery?

- new information for risk re-assessment.

Risk Stage: 4 - Measure - Quality Activities

Mitigation-ID	Mitigation-Description	Unit-Test	Code-Review	Review-Date
M-R-0011-1	Automate data transfer onto transfer media	Verify logic: - Recognition of transfer medium - Data transfer...	- Verify defensive coding - Verify Data types - Verify process logic - Verify correct data state	<Enter Date>

Review-Date = Quality Gate

Review Unit Tests & Code Review

Early indication of:

- progress issues?
- technical complexity?

Risk Stage: 4 - Measure - Quality Activities

Mitigation-ID	Mitigation-Description	SysTest-ID	SysTest-Description	ST Review Date
M-R-001.1-1	Automate data transfer onto transfer media	ST-001.1-1	Verify: - data is encrypted correctly onto transfer media. - data is decrypted correctly off transfer media	<Enter Date>
			Review-Date = Quality Gate Review System Tests Design & Results Early indication of: <ul style="list-style-type: none"> - progress issues? - technical complexity? - defects that require documentation updates? - new information for risk re-assessment. 	

Risk Stage: 4 - Measure - Quality Activities

Mitigation-ID	Mitigation-Description	UAT-ID	UAT-Description	UAT Review Date
M-R-001.1-1	Automate data transfer onto transfer media	UT-001.1-1	<ul style="list-style-type: none"> - Verify the transfer of user equivalent data from "PC A" to "PC B" using correct user roles - Try to run scenario with unauthorized user roles. - Confirm audit trails 	<Enter Date>
			<p>Review-Date = Quality Gate</p> <p>Review UA Tests Design & Results</p> <p>Indication of:</p> <ul style="list-style-type: none"> - progress issues? - technical complexity? - defects that require documentation updates? - updates to operational manuals? - new information for risk re-assessment. 	

Risk Stage: 5 - Repeat - (Report & Act)

Adequate Visibility?	
YES	NO

TASKS
High Level Design (Data Security Performance)
Low Level Design (Data Structures Algorithms)
✓ Design (Review Test Case Design)
Coding (Standards)
Coding (Unit Test)
✓ Coding (Review)
✓ Integration Testing
✓ System Testing
✓ Non Functional Testing (Stress Failover Recover)
✓ UAT (Validation)
Other Activities

Defines My Strategic Approach...

▶ “Create” “Evaluation” “Measure” steps target activities to either reduce issues or identify them earlier: Time - Cost - QUALITY

▶ Reduce defects & Vulnerabilities => HARDEN Software

▶ Information tool - quick visibility on score
makers can then make the call on

▶ Full traceability through

▶ Change Control
requirements

RISK BASED COMPUTER SYSTEM VALIDATION

Physical Design

Test Strategy & Design

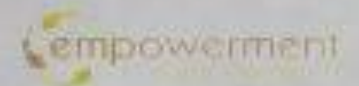
Financial Budget

Quality Feedback

▶ Schedule & cost of the SDLC tasks to be performed

▶ Checks provide early feedback on the quality

▶ Information/evidence to reduce Validation scope



Does it actually work?

Release 1 cost €195k more than Release 2

	Release #1	Release #2	
Pre System Testing Activities (Risk Based)	0	29	More effort, Less cost
System Test	61	48	
Validation	42	4	
Production		0	More effort
Effectiveness		95%	More cost

Less defects =
Less scope for security vulnerabilities =
Reduced window for hackers

Moral of my story...

Keep your hair on ...

... (Critically) Use Risk
Management

Barry McManus

bmcmanus@empowermentqe.com

www.empowermentqe.com

