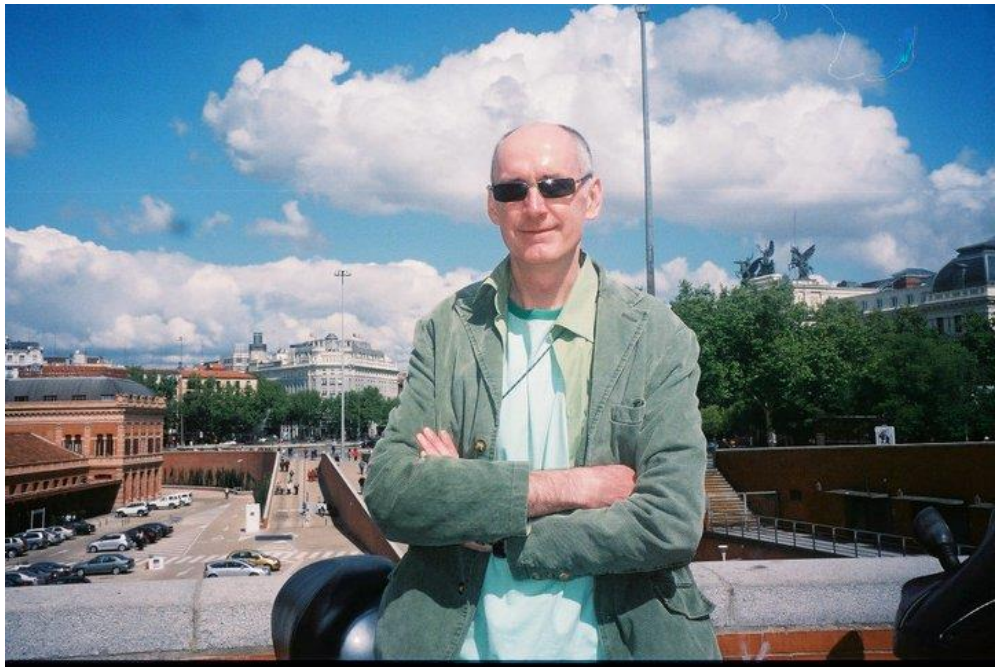
Farewell to “pass or fail”?

James Christie



www.clarotesting.com

blog: www.wordpress.clarotesting.com

James Christie
jack of all trades, master of some

Developer & Business Analyst

Project Manager

Computer Auditor

Information Security Manager

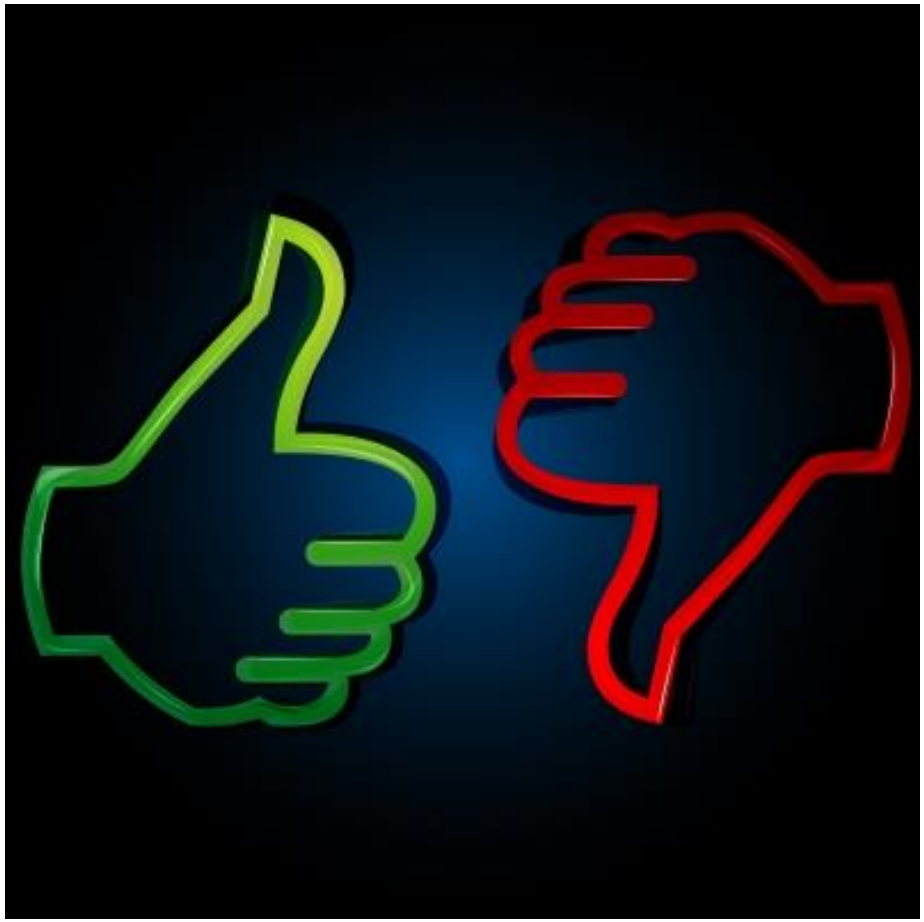
Test Manager & Consultant

investment accountant

trainee chartered accountant

IBM

The Binary Trap



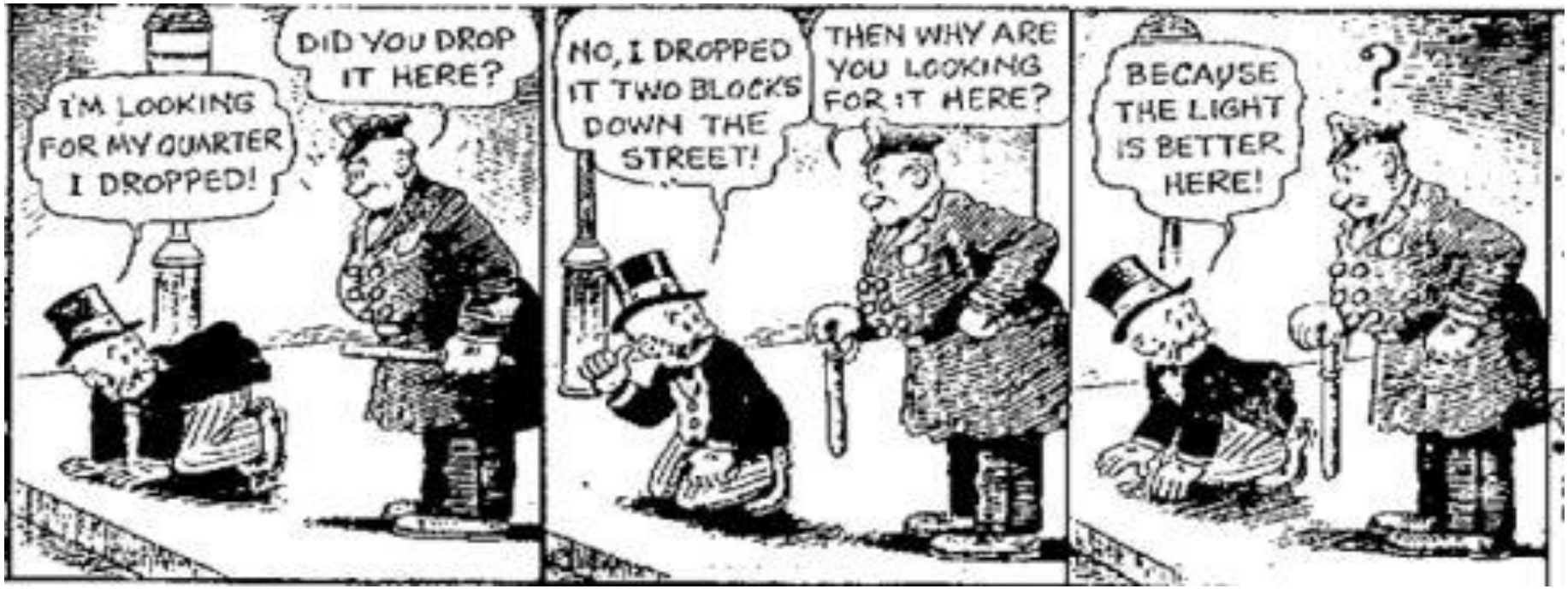
"Reality isn't binary… we don't know everything in advance.

We should observe the software without a hypothesis to nullify."

Rikard Edgren
(see his Oredev talk)

Image courtesy digitalart / FreeDigitalPhotos.net

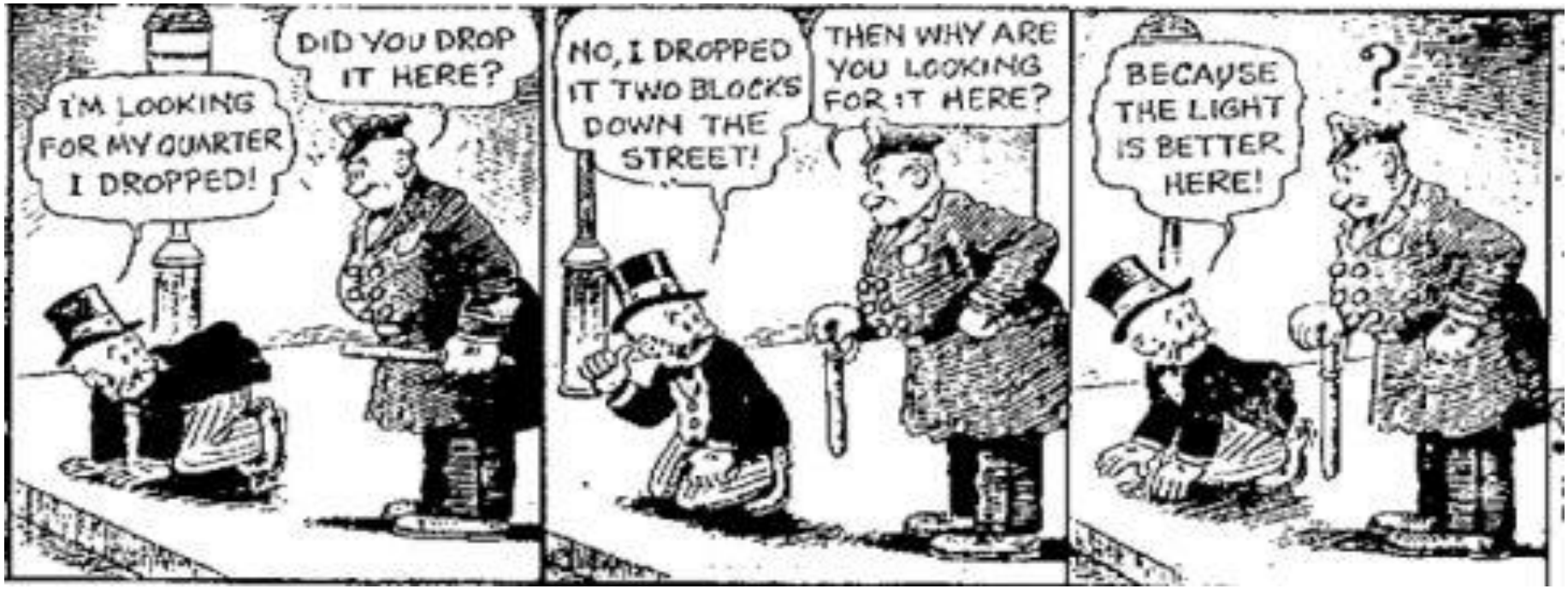
The Binary Trap



The questions we can answer yes/no with most certainty are probably those that don't matter.

The danger is that we focus on them because the light is better there.

The Binary Trap



Ticklists are not auditing.

Test scripts are not testing.

It's not meant to be easy, it's meant to be valuable.

Evidence and Opinion

How do we know anything? What matters? Who cares?

"To know that we know what we know, and to know that we do not know what we do not know, that is true knowledge."
Copernicus

A positivist worldview?

Are we too keen to assume that the world we are investigating is a neater and more ordered place than it really is?

Have we treated testing as if it is like a scientific experiment where we know and control all the variables?

A balanced approach? (just doing the best we can)

We might not know things with certainty, but we can make statements based on evidence & keep refining our opinion.

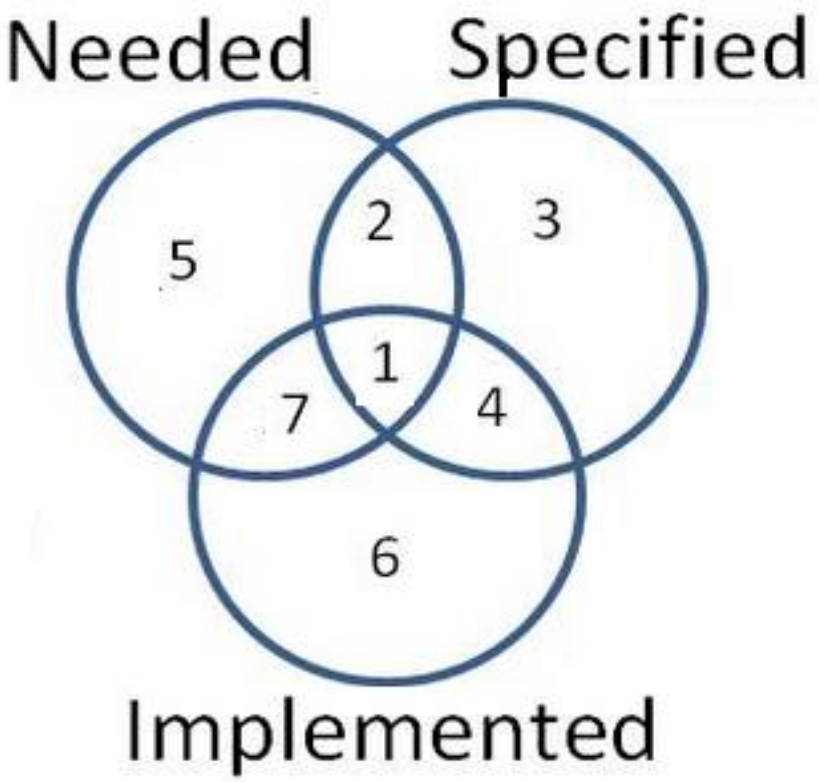
The relevance to testers

Relying on scripts and ticklists assumes that the information we want is under the streetlight.

It assumes that we can know in advance what matters, what we need to look for.

It assumes that the important questions can be answered with a “yes” or “no”.

The relevance to testers and auditors want to know too



If we focus only on what was specified we will not see what was needed but neither specified nor built (5).

And we won't see what was not specified or needed, but was built (6).

Either could be damaging.

Thanks to James Lyndsay, Iain McCowatt, James Bach & Michael Bolton.

What is external audit?

Self image

"… reasonable assurance about whether the financial statements as a whole are free from material misstatement"

"… seguridad razonable de que los estados financieros en su conjunto están libres de incorrección material"

International Standard On Auditing 200
Norma Internacional De Auditoría 200
(applies in EU)

"External auditors are watchdogs not bloodhounds"
English legal case

What is external audit?

"… reasonable assurance about whether the financial statements as a whole are free from material misstatement"

"… seguridad razonable de que los estados financieros en su conjunto están libres de incorrección material"

International Standard On Auditing 200
Norma Internacional De Auditoría 200
(applies in EU)

"External auditors are watchdogs not bloodhounds"
English legal case

Reality

External auditor independence

Challenging client management?

"Commercial suicide"

alleged quote from current chair of UK Financial Conduct Authority.
John Griffith-Jones

Clarification: *"pre crisis, it was not the generally understood role of the auditor to criticise his client's business model and … he might have got short shrift from management for so doing."*

Images courtesy Artur84/FreeDigitalPhotos.net

Big 4 audit fees for 2007

Company	Auditor	Audit Fees ($)
AIG	PwC	97,700,000
Citigroup	KPMG	63,600,000
Goldman Sachs	PwC	49,200,000
Merrill Lynch	Deloitte	45,100,000
JP Morgan Chase	PwC	39,800,000
Morgan Stanley	Deloitte	39,800,000
Bank of America	PwC	39,300,000
Wachovia	KPMG	24,077,600
Lehman Brothers	EY	21,838,000
Wells Fargo	KPMG	17,648,000
Bear Stearns	Deloitte	11,700,000

Source : Audit Analytics

"…fees are now coming before independence, objectivity (and sometimes, even competence) in important parts of the accounting profession."

Paul Moore (ex partner KPMG, ex Head of Group Regulatory Risk, HBOS – 2013)

Images courtesy Artur84/FreeDigitalPhotos.net

Big 6 foul ups in USA

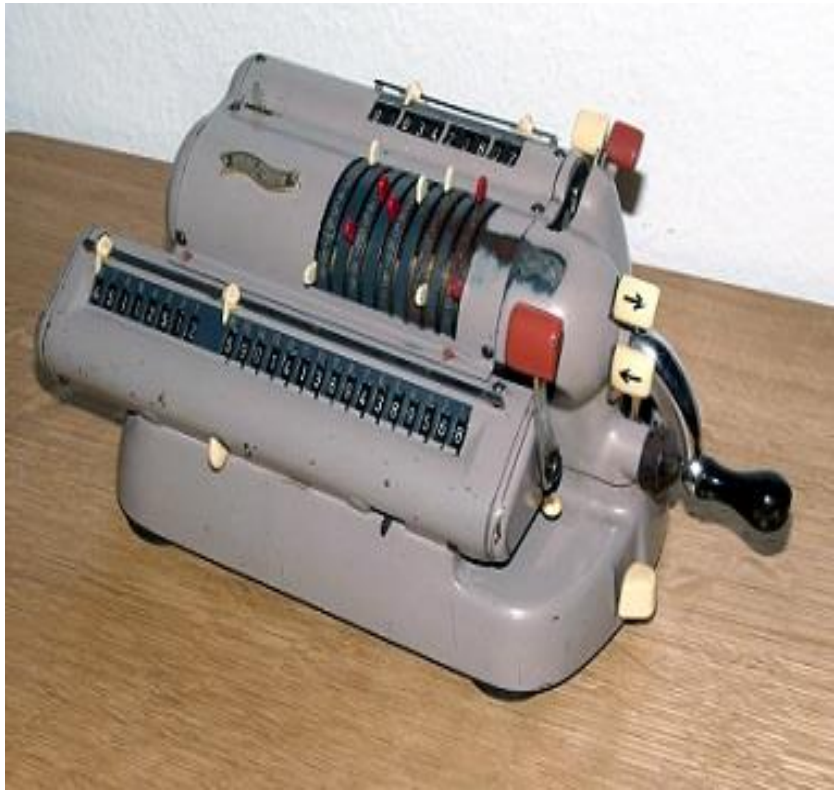
US PCAOB Audit Failures 2012 (2011)

Grant Thornton	65% (43%)
BDO	55% (39%)
Ernst & Young	48% (36%)
PWC	39% (41%)
KPMG	34% (23%)
Deloitte	25% (42%)

(% of audits inspected deemed to be "audit failures" by regulator)

Images courtesy digitalart & Artur84/FreeDigitalPhotos.net

Has external audit had its day?



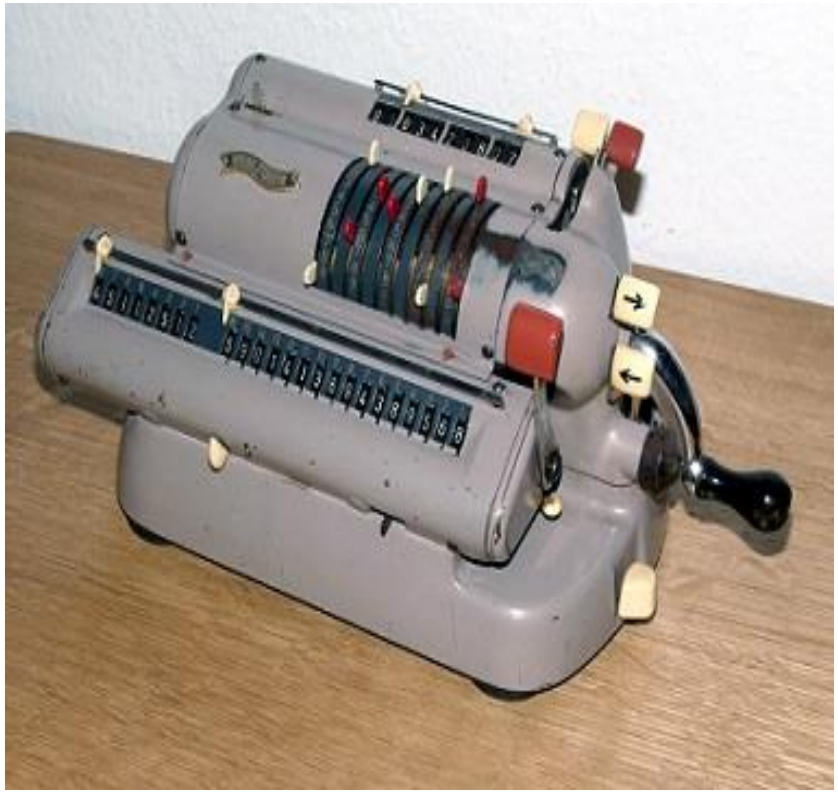
"The fact that the audit process failed to highlight developing problems in the banking sector does cause us to question exactly how useful audit currently is."

House of Commons Treasury Committee "Banking Crisis", 2009

"With or without new rules, the main worry for auditors may be that people wonder whether their reports are worth a bean."

The Economist, April 2014

Has external audit had its day?



"External audit is now largely out-dated. The binary nature of the opinion renders it useless."

Richard Anderson
chairman of the Institute of Risk Management, 2011

"The problem is that there's not a lot of evidence that (external) auditors are very good at assessing risk."

Charles Cullinan, Bryant College, USA

Internal audit – a different perspective

"La auditoría interna es una actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de una organización.

Ayuda a una organización a cumplir sus objetivos pues aporta un enfoque sistemático y disciplinado con el que evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno."

El Instituto de Auditores Internos de España

"Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations.

It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes."

Global Institute of Internal Auditors

Top six qualities internal auditors need

IIA's 2013 Global Pulse of the Profession survey

1 – Critical thinking

2 – Communication skills

3 – Risk management

4 – IT knowledge

5 – Data mining & analytics (fraud! ☺)

6 – Accounting knowledge

Image courtesy cooldesign & FreeDigitalPhotos.net

Internal auditors know more

Deeper business knowledge

Greater tacit knowledge

Greater nous (streetwise, savvy, shrewd, insightful)

More mature, and stronger characters?

Image courtesy Krormrathog & FreeDigitalPhotos.net

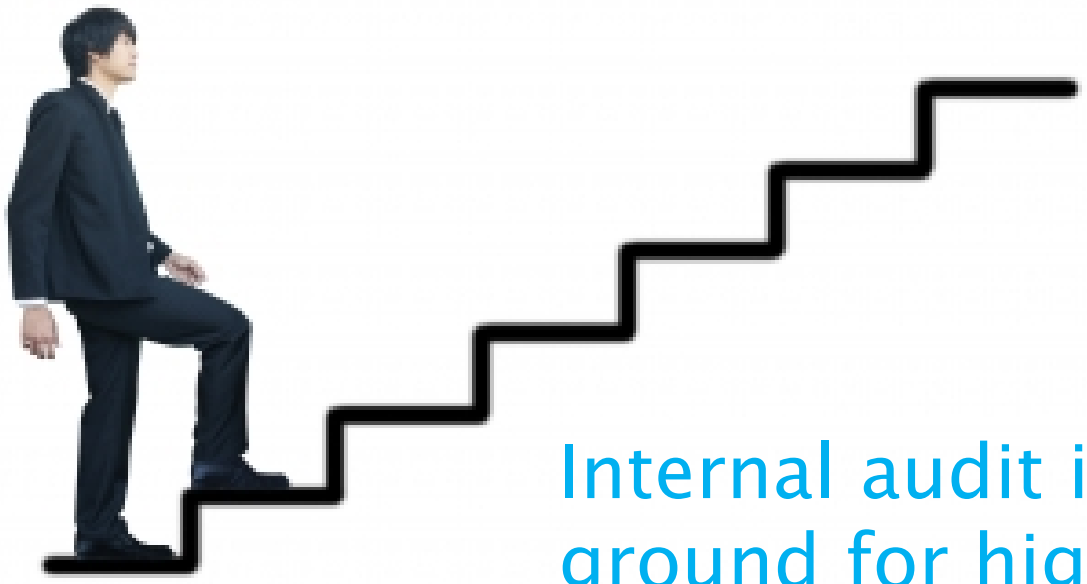
Are internal auditors stronger?

You can't bully good internal auditors.

If you can bully them they don't last long.

Image courtesy Chanpipat & FreeDigitalPhotos.net

The internal audit hothouse



Internal audit is used as a training ground for high quality staff, at companies that take audit seriously.

Risk and the financial crash

Risk is a tricky concept and auditors didn't handle it well.

Image courtesy cooldesign & FreeDigitalPhotos.net

What is risk?

"...the chance, high or low, of somebody being harmed by the hazard, and how serious the harm could be"

(UK Health & Safety Executive)

"the effect of uncertainty on objectives"

(ISO 31000)

"a set of circumstances that hinder the achievement of objectives"

(David M Griffiths, internal auditor)

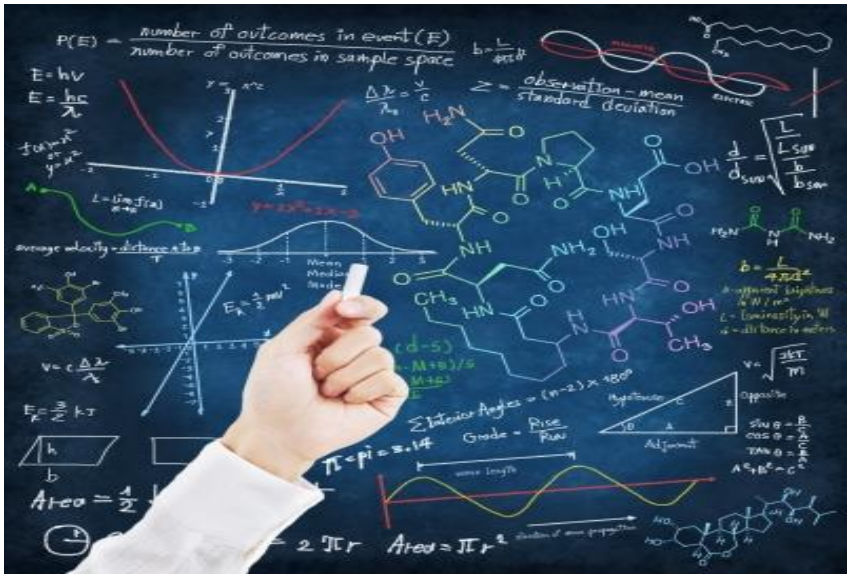
Image courtesy jscreationzs & FreeDigitalPhotos.net

What is risk?

		Potential severity of harm		
		Slightly Harmful 1	Harmful 2	Extremely Harmful 3
Likelihood of harm occurring	Highly unlikely 1	Trivial 1	Tolerable 2	Moderate 3
	Unlikely 2	Tolerable 2	Moderate 4	Substantial 6
	Likely 3	Moderate 3	Substantial 6	Intolerable 9

UK Health & Safety Executive's risk matrix

Risk – the big dilemma



Simple, understandable and totally misleading?

or

Complex, more accurate (possibly) and totally uninformative?

Images courtesy Luigi Diamanti, Mr Brightman & FreeDigitalPhotos.net

Risk – the big dilemma

Rick Buy – Chief Risk Officer.
His stated aim was to *"condense all the risks of the corporation into a single metric."*

ARTHUR ANDERSEN
(it used to be the Big 5)

We lost sight of risk

"With half a decade's hindsight, it is clear the crisis had multiple causes. The most obvious is the financiers themselves – especially the irrationally exuberant Anglo-Saxon sort, who claimed to have found a way to banish risk when in fact they had simply lost track of it."

The Economist, 2013

Image courtesy pakorn / FreeDigitalPhotos.net

We lost sight of risk

"The weaknesses of group risk in HBOS were a matter of design, not accident."

UK Parliamentary Commission on Banking Standards

"An Accident Waiting To Happen: The Failure of HBOS"

Image courtesy pakorn / FreeDigitalPhotos.net

Assurance about risks

Auditors are looking for reasonable assurance, not absolute assurance.

Appropriate…

sufficient…

reasonable…

material

Knowing more about the risks that matter

"Audit priorities (should) align with those of the board and executive management. Risks that keep our stakeholders up at night also should be of concern to us."
Richard Chambers, CEO & President of Institute of Internal Auditors

"The problem is that there's not a lot of evidence that (external) auditors are very good at assessing risk." (reminder!)
Charles Cullinan, Bryant College

Image courtesy digitalart /FreeDigitalPhotos.net

An auditor – one who learns by listening

Good auditors learn by listening

Bad auditors don't listen. Their ticklist tells them the "right answers".

UK & US regulators are pushing auditors away from binary opinions. The EU too?

Attitude of the Institute of Internal Auditors

The Institute of Internal Auditors

Traditional compliance auditing;

"*tipping out the pieces of a jigsaw puzzle on to the Audit Committee table rather than turning those pieces into a picture.*"

Sarah Blackburn, ex President of IIA UK

Image courtesy Stuart Miles/FreeDigitalPhotos.net

Attitude of the Institute of Internal Auditors

Moving this way?

The Institute of Internal Auditors

"In a risk-based approach to security, compliance is provided by security – security is not necessarily provided by compliance."
John Wheeler, Gartner Inc

"Many organizations look at compliance as a set of check boxes… compliance is not the goal, it's a result of securing data in a dynamic and dangerous world."
Mike Rothman, Security Incite

Image courtesy Stuart Miles/FreeDigitalPhotos.net

Attitude of the Institute of Internal Auditors

Moving this way?

Information Systems Audit & Control Association – moving this way?

"the standards committee… define best practice at a point in time, but… best sinks to 'just okay' practice with the passage of time.

A standard is obsolete the day it is published… Carried forward over time, standard practice is mediocrity."

Steven Ross, former ISACA president,
ISACA Journal 2013

Risk Based Auditing

ISACA®
Serving IT Governance Professionals

The Institute of Internal Auditors™

There are no right answers (probably).

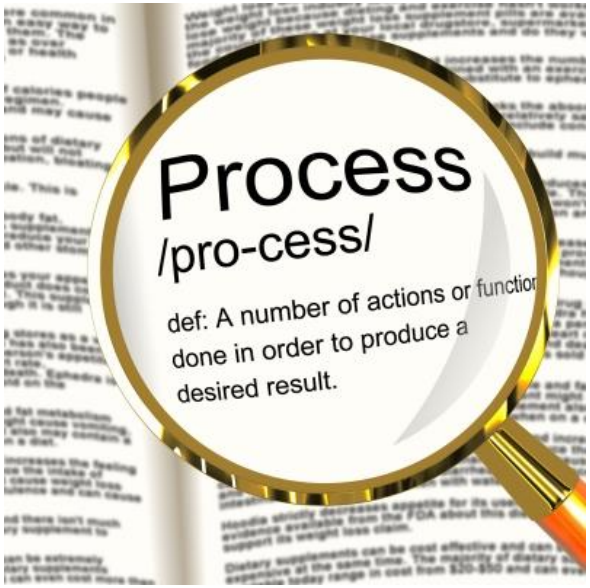
The ticklist is not the audit. It's just a tool.

Auditors who *need* ticklists are unprofessional compliance monkeys. That demeans and deskills the profession.

Image courtesy Stuart Miles/FreeDigitalPhotos.net

Working **with** **good** auditors

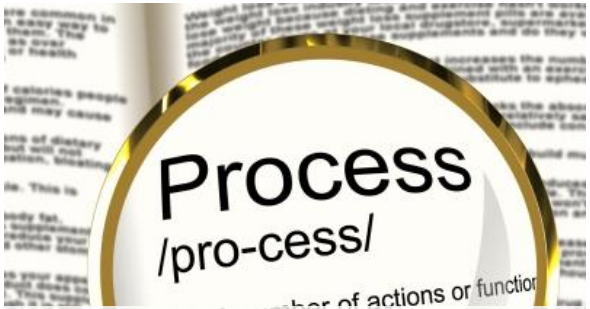
What does a *good* auditor expect?
The same as a good test manager.



Images courtesy Stuart Miles & David Castillo Dominici/FreeDigitalPhotos.net

What do auditors expect from test reports? (with thanks to Rapid Software Testing)

Learning about the product.



But above all – learning about the risks that matter, the risks that keep the stakeholders awake at night.

Learning about how the product was tested.

Learning about how good the testing was.

Images courtesy Stuart Miles & David Castillo Dominici/FreeDigitalPhotos.net

What do auditors expect from test reports?

Don’t empty the box onto the table.

Put the pieces together to assemble a clear picture, to tell a compelling story about the risks that matter.

Don’t try to tell the story by counting the passes and fails.

Image courtesy Stuart Miles/FreeDigitalPhotos.net

What do auditors expect from test reports?

Image courtesy Stuart Miles/FreeDigitalPhotos.net

Auditors live and die by evidence.

Opinions are not casual observations. They must be backed by evidence.

Wrapping up
Get the auditors on your side

Be pro-active. Go and speak to the auditors.

Learn about their concerns. Get their insights into uncertainty, risks and threats.

Learn about their “known unknowns”.

Get their support if you need time, resources and people.

Image courtesy Stuart Miles/FreeDigitalPhotos.net

Wrapping up
Get the auditors on your side

Never follow the letter of the law and ignore the spirit.

Never do something just because “that’s what the auditors will expect”.

Do the right thing and be ready to justify it.

Say what you mean. Mean what you say. **Never** lie!

Image courtesy Stuart Miles/FreeDigitalPhotos.net

Wrapping up

Image courtesy Stuart Miles/FreeDigitalPhotos.net