Plausible deniability

In the film "Independence Day", the President of the United States is taken to a top-secret facility in the desert and shown evidence of alien technologies. Surprised that such important information was kept from him he asks: "Why wasn't I told about this place?" to which the reply comes: "Two words, Mr President: Plausible deniability."

In other words, a person has Plausible deniability when they can deny they knew about something, because they were not told about it, or did not ask a key question, meaning *they genuinely do not know about an important issue, or the lack of action to establish whether there might be an important issue*. The key "benefit" of Plausible deniability is to insulate senior managers and board members from being held accountable for an issue, or lack of action in relation to a risk[1].

Willful blindness

Willful blindness was touched upon in the Enron case when Judge Simeon Lake explained to the jury: "Knowledge [of a fact] can be inferred if the defendant deliberately blinded himself to the existence of a fact". The idea can be traced further back to 1861 in the case of Regina vs. Sleep, where the presiding judge explained that a crucial question to determine the defendant's guilt was whether he "willfully shut his eyes" to a key issue (in this case the origin of valuable property that came into his possession). If he did, he could be found culpable[2].

Whilst these two legal terms have different origins (one from the US and the other from the UK), they are – essentially - two sides of the same coin: with Plausible deniability, a senior leader might be given the benefit of the doubt if something bad comes to light that they did not know about while in charge, but not if it is established that there was Willful blindness on their part.

This article will not discuss the legal technicalities of these concepts, interesting though that is; because that discussion focusses primarily on who might, or might not, be regarded as culpable at a senior level if something goes wrong[3]. Instead we will look at the root causes that can lead to something going wrong in the first place and the broader behavioural factors that result in organizations being blind to what is going on. To do this, I will summarise key research in relation to psychology, neuroscience and systems thinking, some of which may be familiar and some of which may be new to readers. What should emerge is the message that, *even the most disciplined and well managed organizations are prone to be affected by "Predictably Irrational" behaviours, below the surface, at every level*[4].

Drivers of organisational blindness

1: Self-justification and confirmation bias

Anyone in a leadership role and/or with valuable competencies, will appreciate that over time they have developed experience, capabilities and an "edge" to manage more challenging issues. This capability to "see the wood for the trees" builds up one's sense of self-worth, and is also validated by organizational approval, reward and recognition. Nothing wrong with any of that.

In an ideal world, challenges to a leader's judgement should be considered objectively as part of an ongoing mindset to grow and develop and "do the right thing". The problem is that whilst "inconvenient truths" may be an opportunity for learning[5] they can also generate a degree of anxiety: If this challenging fact is true, perhaps I made the wrong decision in the first place? Perhaps the board will think I've lost my edge? And – if this happens too much - I could lose my

[1] The term was coined by the CIA in the years after World War II to describe the withholding of information from senior officials to protect them from repercussions if questionable activities, such as covert operations, became public knowledge. The US Senate Church Committee enquiry of 1974-1975 into intelligence agency activities discusses this in greater depth.

[2] See the excellent book "Wilful Blindness" by Margaret Heffernan.

[3] Focussing attention narrowly at the top of organisations, and not considering wider behavioural and cultural factors.

[4] See Dan Arielly's book: "Predictably irrational."

[5] Remembering different levels of learning – explained well in the double-loop learning model by Chris Argyris.

position and status! (I make these statements in the extreme form to stress the underlying dynamic).

As a defense against self-doubt, we have the psychological phenomenon of "self-justification", which is a tendency to defend what one has already done[6]. Alongside this, we have "confirmation bias" which is the tendency for people to prefer information that confirms what they already think, and to ignore, or downplay, information that challenges their existing view[7]. In fact, people are twice as likely to prefer information that confirms what they already believe, rather than to accept something that suggests the opposite[8].

2: Group dynamics and behavioural change in relation to authority

We must all have attended a meeting expecting a burning issue of concern to be discussed and then observe that it is raised in very mild tones, (and consequently not picked up with any vigour by others); or not even brought up in the first place[9]! The psychological factors in play include a tendency to want to fit in with a group, and not rock the boat, as well as a preference to follow the lead of an authority figure. Classic scientific experiments have measured these phenomena – amounting to as much as 33% tending to group conformity (see papers by Solomon Asch) and 66% in relation to "obedience to authority" (see papers by Stanley Milgram[10]).

Of course, there are always examples of teams and committees that are truly open and honest, where leaders and chairmen welcome challenge and members are free to speak their minds; but the default for many is to hold back what they are thinking because of real or imagined pressure from others[11].

To understand this better, Gregory Berns at Emory University has demonstrated, by looking at MRI scans of those involved in group perception exercises, that *there was no activity in the prefrontal cortex in some participants of a group when they were aware of what other participants the group were thinking*[12]. In other words, knowing what the group thought changed what the participants saw; indeed, they became – unconsciously - blind to what they were seeing.

Note also that the cultural tendency in many organizations to value good team players, and look for good team spirit as a mark of potential and cultural fit. However, it is important to recognize that this could equate to a culture that prefers conformity and comfort over thinking and challenge; resulting in issues that are in plain sight being missed. Getting this balance right is a key cultural challenge for many organizations.

3: Organisational complexity, unclear roles and accountabilities and distance

An added dimension of why organizations can be blind to important information stems from the "Bystander effect"[13] in which the presence of others can reduce the likelihood of others to investigate what is happening and/or act (i.e. if they aren't doing anything, why should I?).

Furthermore, the complexity of many modern organizations, often separated into specialist departments and each with their own specific objectives, can drive "silo" behavior. In the context of GRC activities, the people that write policies and standards are invariably not the people who have to implement them. In my experience, a lot of corporate governance theatre derives from the fact that, from a top down perspective, policies and standards are in place, but in the messy reality of day to day organizational life, staff barely have time to read all the policies and standards that apply to them, let alone have the time to fully implement them! And when staff are

[6] See "Mistakes were made, but not by me" by Carol Tavris and Elliott Aaronson.
[7] Readers will be evaluating this article through this filter: if you agree with what I am saying you will be satisfied; if you do not agree you will be thinking of examples that contradict what I am saying.
[8] Research by University of Illinois psychology professor Dolores Albarracín, with University of Florida researcher William Hart.
[9] Even though it may have been discussed informally for some weeks!
[10] Which was replicated by Derren Brown in 2006 in the TV special "The Heist"
[11] See Elliott Aaronson.
[12] http://www.ccnl.emory.edu/greg/Berns%20Conformity%20final%20printed.pdf
[13] Coined after the killing of Kitty Genovese in front of dozens of people in New York City in 1964.

asked whether things are alright, they will invariably say that they are, in part because of confirmation bias, and/or out of a desire to satisfy the expectations of authority figures!

These considerations can drive a culture summed up by the maxim: “When it goes well, we want to take the credit; when it goes badly, it was someone else’s fault”.

Success: Everyone claims the credit

Failure: Was someone else’s fault

So far we have identified some of the psychological drivers that lead to organizations being blind to issues and risks, as well as other factors that can contribute to not passing on bad news and not asking probing questions. Beyond this there are two other dimensions of note that contribute to organizational blindness:

4: Resources, dilemmas and challenges with priorities

Excepting a few clients I have worked with in the Middle East, there are few that say they have enough resources to do all the things they want, at a strategic and/or at an operational level. Therefore, most managers and staff are given a range of objectives which cannot all be achieved with the resources available. Some of these will be business or delivery related objectives, and others will concern being compliant/“in control”, or improving GRC. Consequently, one of the defining skills of any good manager is learning how to juggle priorities and make sure that key things get done[14]. An analogy is to envisage a circus performer with numerous spinning plates on sticks; ideally they will stop any from falling; but if one does fall, it had better not be one of the most valuable plates[15]!

That said, countless disasters can be traced back to the problem of: i) insufficient resources allocated towards GRC activities and/or, ii) GRC activities not given sufficient priority against the backdrop of other business/service delivery objectives.

The BP Texas refinery explosion and fire of 2005 provides a chilling illustration of this problem in practice. Despite numerous safety incidents, including fatalities in 2004, there were nonetheless blanket cost cuts imposed. Prior to a meeting to discuss budget cuts at the Texas facility, one manager sent the following email: “Which bit of 25% don’t you understand? We are going to be wasting our time on Monday discussing this topic unless you come prepared to commit to a 25% cut. I have much more interesting things to do with my time that getting up at 3am [..] for a non-productive meeting!”.

Note that the need to manage budgets and manage cost targets is not the biggest issue here; every organization needs to be financially responsible. The problem is *a culture in which discussing stretching budget targets, dilemmas around choices, the tough decisions to be made,*

[14] And it is one of the reasons I became interested in lean and agile ways of working.

[15] See the “Monkey business illusion” video for a fun example of how easy it is to miss key things.

and the consequences of these, is not possible. Silence around issues that everyone knows about, but no one is prepared to bring up, is one of the key cultural indicators that there is organizational myopia, and therefore surprises and disappointments may not be far away[16].

5: "Foxy" managers and organisational politics

One of the areas I support GRC and audit professionals is in relation to enhancing their political savvy. To facilitate discussion, I use are the ideas in the paper by Simon Baddley and Kim James: "Owl, Fox, Donkey or Sheep: Political Skills for Managers". Even though this paper was written in 1987, the insights from their research are not widely known[17].

Their research shows that political adeptness is one of the essential skills needed to rise to the top of an organisation, and to stay there. Thus, sheep and donkeys are unlikely to rise to senior levels because of a lack of political skills, and instead, senior managers are comprised almost totally of owls or foxes, both of whom have political astuteness[18]. The difference between the two is that the owl is motivated to do the right thing for the sake of the organisation, whereas foxes are principally concerned with doing what's needed to acquire or maintain their personal power and influence.

To complicate things further: i) one of the key skills of a fox is to pretend to be an owl[19], ii) few organisations openly recognise organisational politics is a widespread and inevitable part of organisational life, and iii) fewer still equip their staff with the skills to recognise and deal with "foxy" managers!

So now we come back to the place that we started: Plausible Deniability / Wilful blindness etc. are tools that may be used by "foxy" managers to protect them from blame! However, the problem of their deliberate blindness should be seen in the context of the many ways that staff and managers are blind as well. It takes a lot of people to collectively miss things, or downplay things, or remain silent, before a corporate disaster happens.

Practical ways to address organisational blindness

Readers who have followed the discussion up to this point should be aware that I am not about to come up with a "magic bullet" that will address all the problems outlined; and the more political the organisation[20], the less it will welcome what I am about to say! That said, typical areas that can be improved are as follows:

A: Tighten up disciplines concerning Self Assessments
My good colleague Dr. Mannie Sher[21] summarises the problem: "There is only one problem with Self Assessments – the Self."

Consequently, *any process that requires self-assessments from managers[22],* or assessments that risks are being well managed, *should assume that some optimism bias may be present,* not least where foxy managers are involved[23]. Therefore, questions should be focussed, criteria for assessments should be crystal clear, and *if the manager says everything is fine, they should be asked to state, for important issues, what evidence they have to confirm that this is the case*

[16] See Chris Argyris on: "Organisational defence routines"
[17] The reasons the paper is not well known are understandable when you read the paper; self-interested, politically adept ("foxy") managers, who are often in positions of power, are unlikely to embrace a framework that names them and identifies their ways of working to others, who may be less politically aware and adept.
[18] The paper sets out the different types of person in more detail, but a common-sense approach to what these terms mean is sufficient for this high-level discussion.
[19] Although there are invariably subtle signs that give them away.
[20] Political levels range from: Minimally political, to moderate, highly political and finally: pathologically political – see various books and papers by Kathleen Kelley Reardon.
[21] At the Tavistock Institute.
[22] For example: confirmations that a department is compliant with laws and regulations or up-dates on progress against targets (especially where there is an element of judgement).
[23] This is also a reason that it is important at the start of any audit to be clear which issues have been identified by management and are being acted on, and to make this clear when reporting the results of the assignment.

(beyond having a string of other self-assessments from their staff). Some organisations further strengthen the robustness of self-assessments by requiring documentation and evidence to be stored securely on-line, so that it can be reviewed in more detail by senior managers, and/or risk/compliance/audit[24].

The Chartered Professional Accountants in Canada paper "A framework for board oversight of enterprise risk[25]" highlights that boards need to better recognise that senior executives can be attached to certain business development initiatives for personal reasons[26]. It explains that the more this is the case[27], then more the board should carefully analyse what is being proposed, and be vigilant in relation to over-optimism and the down-playing of risks.

In relation to audit and assurance, the IIA UK has produced a very good paper: "Effective internal audit in the financial services sector."[28] It highlights that internal audit should be able to review "the information presented to the Board and Executive Management for strategic and operational decision making", implicitly recognizing that the information presented to the board and executive management may contain bias or gaps, and that these might be revealed if the information and assumptions are pressure tested by internal audit[29]. I would urge those not familiar with this paper to read it, since it sets out what a modern, effective, internal audit function should look like (and is transferrable to audit functions in many domains, not just financial services).

B: Proactively manage for group dynamics and behaviours around authority figures

Following the 2007-2008 financial crisis, the Walker report recommended a range of measures to reduce the likelihood of similar issues in future[30]. Annex 4 of that report expands upon the group dynamic issues mentioned earlier, and highlights the importance of skillful chairing of the board to minimize the effects of these forces[31]. For the reasons discussed in this paper, these recommendations are equally valid for organizations that are not in financial services[32]. Moreover, understanding and managing group dynamics applies to *all management teams, project teams and board sub-committees in an organization (such as Risk, Remuneration, Audit*)[33]. And any reader who thinks that the committees and management teams they work on do not have group dynamics, or room for improvement in the way they work, has, I regret to say, almost certainly become blind to this.

In the specific context of risk management workshops, clients of mine *collect information about risks in advance of any meeting on an anonymous basis to allow "inconvenient truths" to come to light without group pressure to suppress them*. Leaders are also coached on ways to allow management teams to develop their preliminary conclusions without overly steering what gets proposed.

Likewise, some risk owners, compliance and risk functions and audit functions play an important challenge role in relation to risk assessments for critical and strategic risks. They understand

[24] Which signals that the self-assessment process is serious and not just to "tick the box."

[25] https://www.cpacanada.ca/en/business-and-accounting-resources/strategy-risk-and-governance/enterprise-risk-management/publications/a-practical-approach-to-board-risk-oversight

[26] Beyond fraud, and more for the status such a project may provide.

[27] Defined: Level 1 and Level 2 depending on the likely degree of attachment / risk of bias.

[28] https://www.iia.org.uk/resources/sector-specific-standards-guidance/financial-services/financial-services-code/

[29] Or other Independent Assurance providers. Note that consultants who are asked to support a proposal/project may have a conflict of interest in relation to being completely transparent about key risks because of future fee income that they may get if a proposal/project is approved.

[30] http://webarchive.nationalarchives.gov.uk/+/http:/www.hm-treasury.gov.uk/d/walker_review_261109.pdf

[31] Co-authored by Mannie Sher and Alison Gill

[32] Which is why there is a growing recognition of the need to have board evaluations by experienced consultants across all sectors.

[33] In other words, a board may be high functioning, but fail to fully see dysfunctions in key management teams where they are not present.

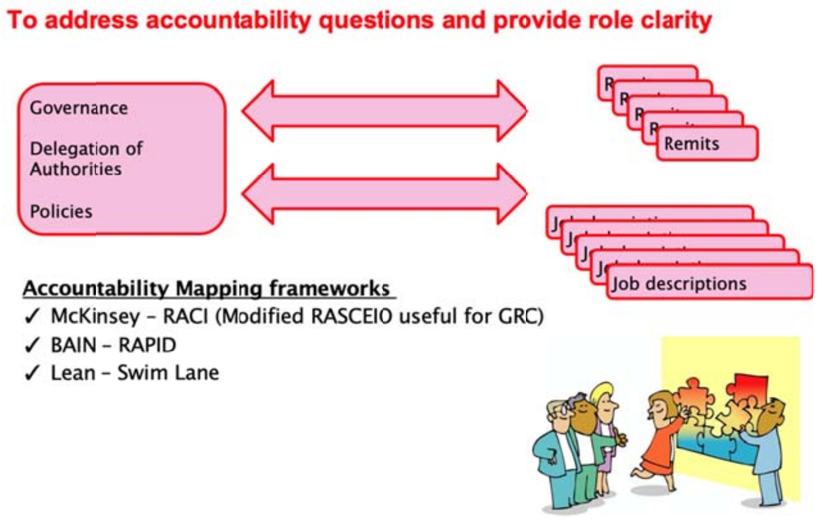
that, no matter how well they try, a collective assessment by a project team, management team or committee may none the less be missing important risks, or key mitigating actions[34].

C: Drive a culture of clearer roles and accountabilities, using an accountability mapping tool.

Well-defined roles and accountabilities are fundamental at the top of any organization, and this is an area that has been tightened up in the UK Financial Services Sector[35]. Readers should note that this "senior management regime" is not yet applied across all sectors in the FTSE, even though there are many large UK companies, not in financial services, where unclear accountabilities and competency gaps have, and could, result in significant damage to the economy[36].

That said, accountabilities at the top are normally well articulated in many companies with a well-functioning board. However, below accountabilities at the executive level, I regularly encounter complexity and confusion in relation to roles and accountabilities. For example, for a cross-functional process or system, there *may* be a defined process or system owner[37], but there can still be issues around hand-overs between functions because of unclear roles and responsibilities at an operational level.

To address roles and accountabilities at a practical, operational, level Accountability Mapping Frameworks are an invaluable tool[38]. These provide an excellent "half way house" between committee remits, and high level policy statements about roles, and individual job descriptions and targets. Accountability mapping is a key way to reveal "hairline cracks" concerning who does what, that may be suspected, but have not yet been pinned down. Such mapping tools address the common problem: "This is a job that should be done by everyone, which in practice means it's a job done by no-one"[39]


To address accountability questions and provide role clarity
Governance
Delegation of Authorities
Policies
Remits
Job descriptions
Accountability Mapping frameworks
✓ McKinsey – RACI (Modified RASCEIO useful for GRC)
✓ BAIN – RAPID
✓ Lean – Swim Lane

Accountability Mapping is also invaluable when considering the way that critical and strategic risks are assessed, as well as when working on risk assurance mapping[40]. In addition, it is a

[34] Best practice is "Risk based risk management", where the most important risks of an organisation are thoroughly pressure tested.
[35] https://www.fca.org.uk/news/speeches/culture-conduct-extending-accountability-regime
[36] Think about the size of the recent Carillion collapse in the UK
[37] Although the detailed tasks that must be carried out by the process/system owner may be rather vague, especially in relation to overseeing the work of other functions, or not.
[38] Three key accountability mapping frameworks are: Lean – Swim Lane; Bain – RAPID and McKinsey RACI.
[39] Remember the "By-stander effect" and remember foxy managers are happy to exploit these ambiguities in roles.
[40] Risk assurance mapping helps to clarify assurance roles between different functions, especially "who audits what." Note also that just because someone has the job title "Head of Health & Safety", "Head of Legal" does not mean they will agree they are ensuring that these risks are "in control".

useful tool that can and should be used by Internal Audit teams to make visible issues with roles and accountabilities, also providing a framework to facilitate their timely resolution[41].

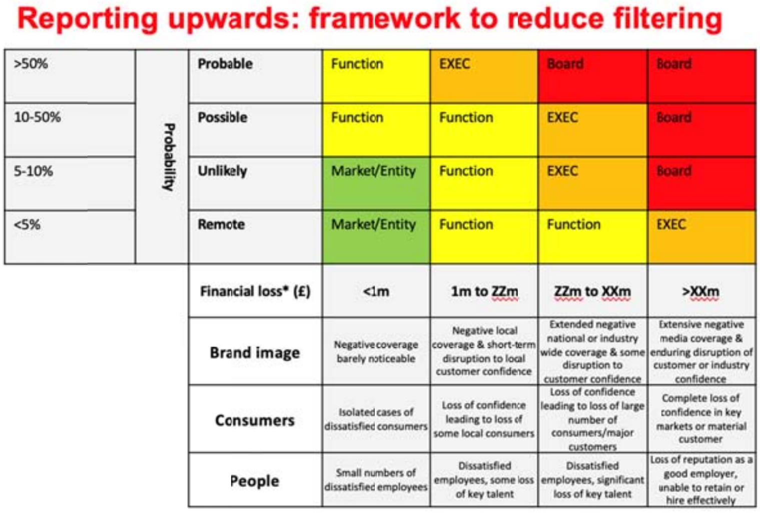
In relation to policy development and roll-out, senior managers and board members should *ensure that any policies and standards developed have been meaningfully discussed with operational managers and staff, to be confident that policies are clear, and can be implemented at a practical level*. In addition, accountabilities for developing training materials, tracking training and following up etc. are vitally important to pin down for key policy areas[42].

<u>D: Ensure priorities and challenges with resources are openly discussed, and demand upward reporting without filtering or delays.</u>

As discussed, resource dilemmas and competing priorities are an inevitable fact of organizational life. However, these can become corrosive, and create risk surprises, when it becomes difficult or impossible to discuss these constraints openly.

Consequently, board members should ask senior managers to "be real" about resource pinch-points. For example, forecast and budget discussions, as well as risk management processes, should explicitly address risks *caused by cost pressures and change initiatives,* and how these might be managed, not simply the risks to delivering objectives and change projects[43].

Mechanisms to promote greater openness include clearly defined key risk indicators and tolerance levels for key risks, so that filtering or "playing for time" in relation to upward communication is not tolerated. The framework below, developed for one of my clients, illustrates at a practical level how to encourage early reporting upwards. Note that potential impact is the main influencer for reporting upwards, even if the chances of a problem are remote.



Reporting upwards: framework to reduce filtering

>50%	Probability	Probable	Function	EXEC	Board	Board
10-50%		Possible	Function	Function	EXEC	Board
5-10%		Unlikely	Market/Entity	Function	EXEC	Board
<5%		Remote	Market/Entity	Function	Function	EXEC
		Financial loss* (£)	<1m	1m to ZZm	ZZm to XXm	>XXm
		Brand image	Negative coverage barely noticeable	Negative local coverage & short-term disruption to local customer confidence	Extended negative national or industry wide coverage & some disruption to customer confidence	Extensive negative media coverage & enduring disruption of customer or industry confidence
		Consumers	Isolated cases of dissatisfied consumers	Loss of confidence leading to loss of some local consumers	Loss of confidence leading to loss of large number of consumers/major customers	Complete loss of confidence in key markets or material customer
		People	Small numbers of dissatisfied employees	Dissatisfied employees, some loss of key talent	Dissatisfied employees, significant loss of key talent	Loss of reputation as a good employer, unable to retain or hire effectively

<u>E: Drive a culture of greater openness about organizational politics, to reduce the cover for "foxes" to hide.</u>

It is outside the scope of this article to do justice to the fascinating topic of organizational politics, and how to manage foxy managers. Recognizing foxy behavior is the starting point to develop skills in political savvy. However, specific strategies and tactics concerning what to do to counter

[41] HIAs should consider including a RASCIEO chart as an appendix to an audit report where accountabilities may be an issue.
[42] In other words, we need a better way of defining what we mean to "roll-out" / implement a policy. An invaluable practical framework is the "7 elements of an effective compliance framework", published by the US OIG.
[43] Cost savings programmes are invariably initiated to address one risk (i.e. excessive risks), which can give them a "halo" effect that blinds management to their negative consequences. A good risk culture can see both sides.

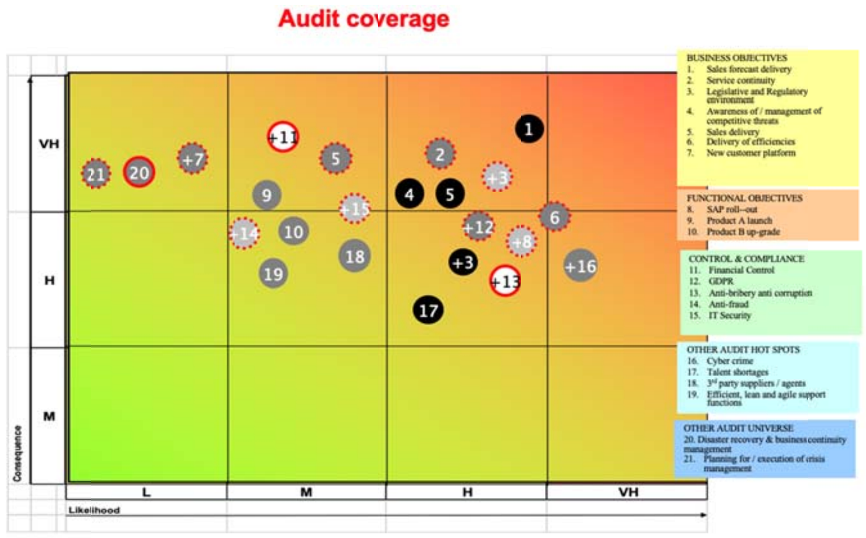
dysfunctional politics will be specific to each organization, its context, the foxes who are in positions of power, and whether there are any owls around![44]. And even if one understands politics in theory, it also takes time and practice to become skilled in this field[45]. It may seem to be a paradox, but as I see it, *management training and development on political skills should be part of the core curriculum for any organization that wants to reduce political dysfunctionality*[46].

In general, strong processes, and a culture that seeks transparency around exceptions and variations, can play a useful role in stopping foxy managers from finding and exploiting “escape routes”. Another way that foxy managers work is to influence internal audit teams to audit areas that will embarrass other managers – effectively using audits as weapons. In this context, internal auditors should be mindful why some areas have been requested for an audit and check carefully the expectations senior managers have in relation to the outcome of the audit. Audits on known issues, or where there is a clear expectation that someone should be blamed[47], should be accepted with great care[48].

There are three key areas where transparency in the audit plan is important:

i) Making it crystal-clear which areas are audited regularly, and which areas are “no go zones”[49];
ii) Being clear about the amount of “reasonable assurance” that will be provided[50];
iii) Being clear about others who are accountable for providing assurances[51]

The table below provides an illustration of the ways in which internal audit coverage against key risks and objectives can be made transparent to senior executives and the board. The aim is to make it more difficult for no-go zones to be hidden, which is what foxy managers prefer. Note that this format, which I used when Head of Internal Audit, also highlights how resources are affecting the total audit coverage of key risks – only the risks highlighted in red will be audited or reviewed.



[44] Michael Jarrett discusses the importance of Political Terrain in his HBR article: “The 4 types of organisational politics”.
[45] Through coaching and other techniques, such as “Action Learning”
[46] I view training on political savvy and how to deal with foxes as the equivalent of the “Defence against the dark arts” training that will be known to followers of Harry Potter.
[47] Or scapegoated, a common “foxy” manager trick.
[48] This can also include situations where audits in the audit plan are effectively a weapon of the audit committee towards executive management; often reflecting a deeper issue of a lack of trust between the two groups.
[49] The diagram represents risks regularly audited (in white) and areas never audited (in black).
[50] Distinguishing between audits: all key risks and substantial testing (solid red circle) and reviews: sellected key risks and some probing (dotted red circle).
[51] Other assurances (e.g. Health & Safety, Compliance, IT security etc.) denoted by +

F: Tighten up disciplines in Root cause analysis, remediation timescales and ratings criteria.

It should be clear from all that has been said before, that organizations that are serious about avoiding GRC surprises should pay careful attention to the underlying root causes for problems, not just the immediate and contributing causes. Internal Audit teams should strengthen their capability in this important area, but this should be part of a journey in which all key functions get better at analyzing why things are going wrong, without scapegoating individuals[52].

Foxy managers can be masters at agreeing to audit actions and then doing the bare minimum, invariably asking for extensions to deadlines at the last minute. For this reason, there should be a clear framework agreed concerning how long managers can have to remediate actions. Such a framework must balance the dilemma that important issues should be remediated as quickly as possible, but at the same time, important areas are invariably the ones that need the most resource to be properly fixed. A good risk culture demands regular discussion about speed/quality/resource challenges in relation to risk and audit action planning.

In addition, the remediation process itself should be made more "fox proof" by, for example, setting interim milestones. For example, if there is a 9-month target to implement an automated control, there might be interim targets agreed, and tracked as follows: Create new process ~ 3 months; Define new system requirements ~ 6 months; Go live with new system ~ 9 months. Each of these milestones should then be tracked, so that slippage can be made clear much earlier.

Finally, audit ratings should be carefully considered to ensure they do not drive dysfunctional behaviors. One dysfunction is to demand "No Unsatisfactory ratings", which typically results in less openness from managers, and results in time-consuming arguments about ratings. Another dysfunction can be where most audit ratings are in the middle of a spectrum and – in practice – the organization becomes "comfortably numb" to most ratings, except where they are very bad.

I believe there are at least two hallmarks of good practice in relation to audit ratings:

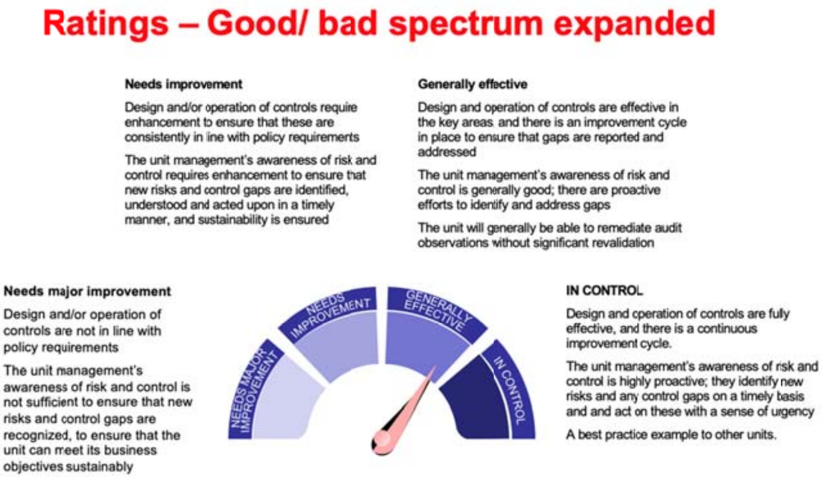
I) Distinguish clearly between "How big" and "How bad" when rating what has been found[53];

II) Be mindful when the best audit rating is just "Good" or "Satisfactory".

On the latter point, a good practice is to *reserve the best audit rating for truly excellent/leading practice*. Such a change in ratings will have the effect of reducing considerably the number of top ratings and will tend to drive a culture that is less complacent around risk and control matters. The table below provides a summary of such a progressive audit ratings framework:

[52] I have recently run several Root Cause Analysis workshops with Audit, Risk, Compliance and other functions in attendance.

[53] This was implemented in AstraZeneca and cited as a good practice by the Audit Director Roundtable, since it i) avoided diluting adverse ratings because they were lower impact and ii) allowed for a more mature discussion about control effectiveness against good practice, separate from the question of the impact on the organisation.



Ratings – Good/ bad spectrum expanded

Needs improvement

Design and/or operation of controls require enhancement to ensure that these are consistently in line with policy requirements

The unit management's awareness of risk and control requires enhancement to ensure that new risks and control gaps are identified, understood and acted upon in a timely manner, and sustainability is ensured

Generally effective

Design and operation of controls are effective in the key areas and there is an improvement cycle in place to ensure that gaps are reported and addressed

The unit management's awareness of risk and control is generally good; there are proactive efforts to identify and address gaps

The unit will generally be able to remediate audit observations without significant revalidation

Needs major improvement

Design and/or operation of controls are not in line with policy requirements

The unit management's awareness of risk and control is not sufficient to ensure that new risks and control gaps are recognized, to ensure that the unit can meet its business objectives sustainably

IN CONTROL

Design and operation of controls are fully effective, and there is a continuous improvement cycle.

The unit management's awareness of risk and control is highly proactive; they identify new risks and any control gaps on a timely basis and and act on these with a sense of urgency

A best practice example to other units.

Summary

To conclude: Consider the analogy of flying an aircraft. You are the pilot and 100 flights have gone well. Do you stop checking the fuselage for hairline cracks? Do you omit to check whether a repair has been done? Do you ignore what the fuel tank gauge says? Do you ignore whether the radar and intercom are working? Do you dispense with the pre-flight checks?!

The reason we don't dispense with these checks is because if we go up in a plane, and get it wrong, we might die. Whereas if our organization loses money etc., it's often not our personal money that is taken away! Such asymmetries are common place[54] and are often accompanied by the "blame someone else" culture.

So, the message should be clear, ongoing vigilance by all lines of defence[55] of an organization, recognizing the ongoing possibility of myopia, and the sharing of specific good practices, is the only sensible mindset to have to reduce the chances of a major risk surprise.

James C Paterson has been a GRC and audit consultant since 2010. He delivers training for 12 of the Institutes of Internal Audit in Europe. He has a Masters degree in management, specializing in cultural issues, and spent two years working in HR for AstraZeneca, before becoming Head of Internal audit for AstraZeneca for seven years. He has spoken at three recent international IIA conferences, and has been the Chairman of the European Union Internal Audit Service Conference for 2017 and 2018. He wrote the book "Lean auditing" in 2015, published by J Wiley and sons. Website: www.RiskAI.co.uk.

[54] See the latest book by Nassim Nicholas Taleb: "Skin in the game"
[55] 1st line ~ Management; 2nd line ~ policy and compliance functions; 3rd line ~ independent assurance (including internal audit)