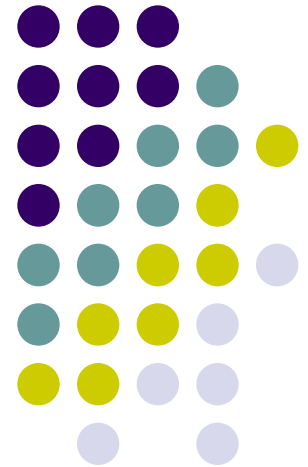
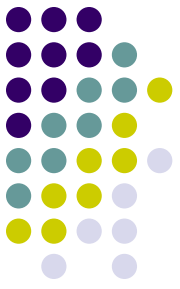


IT Audit Traps for New Players

Yvette Polonyi



IT Audit – Traps for New Players

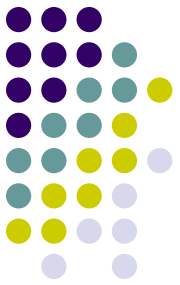


- An IT project is like any other.
- IT Managers are always too busy to meet with auditors.
- We (auditors) have the authority to audit this area – they must allow access.
- We know more about how to control processes than the client.
- They must implement the audit recommendations.
- These IT types are just trying to confuse me with jargon.

An IT project is like any other?

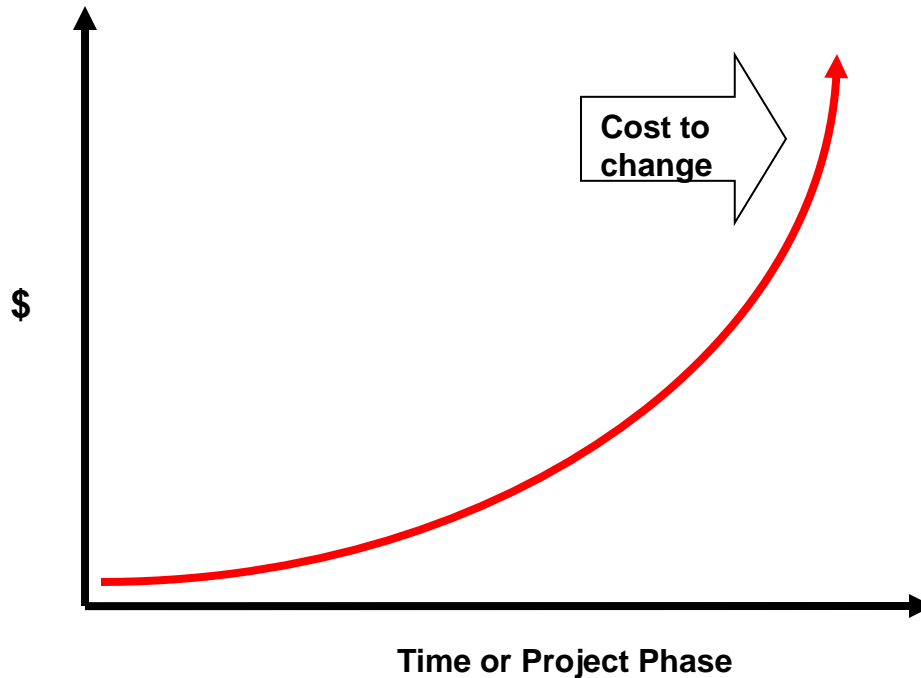


- At least 70% of IT projects fail: i.e. do not deliver on-time in-budget, and to client satisfaction.
- Complexity.
- Business requirements are not static.
- Users can be unpredictable.
- Emotional investment in IT projects.



Cost over time...

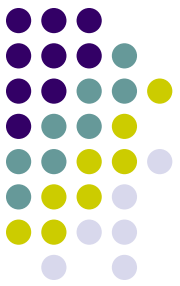
- The rule of exponentially increasing cost to change systems over time:



CIO's & IT Managers

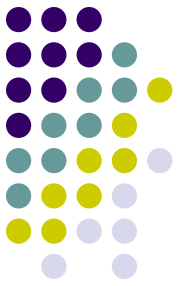


- “How accessible are you to auditors?”



How accessible?

- Quite. Many audits are useful, and I am very engaged. All recommendations are tracked and reported to the Executive.
- Very. Same for internal audit and ANAO.
- I make myself accessible to audit. I am more conscious of ANAO!
- Auditors need to be in communication with IT when developing the Annual Audit Plan to **add value**.



How accessible?

- I am completely accessible and take audit very seriously. Internal, ANAO – same.
- Always accessible – audits add value.
- I have requested audits where additional “set of eyes” may assist in addressing systematic problems.

CIO's & IT Managers

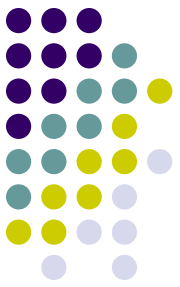


- “What do you expect audit to do, in order to gain access to you or your area?”



What does audit have to do?

- Build trust: All on the same side & want to achieve the same outcome. But audit doesn't have so much skin in the game!
- ICT projects fail because people get too close. **If you're going to fail, fail early and fail cheap!** (Culturally not there, but audit can give focus.)
- I engage with internal audit in order to get value.



What does audit have to do?

- Communicate, make appointments.
1st at a high level to discuss scope, provide status of the project and where audit may provide most value.
- Devise and agree an audit.
- Provide a clear understanding of terms of reference before the audit (to allow planning).
- Clear indication of what audit will need from staff, including time (to allow scheduling).

What does audit have to do?

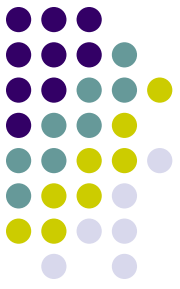


- Not everything is immediately accessible.
- Preferable to provide as much as possible at the outset.
- Auditors should explain the audit to staff on Day 1.
- Have a sensible work program.
- Willingness to negotiate and listen. A solution may not be so simple: Pragmatic vs. theory.
- Not after the fact.

CIO's & IT Managers

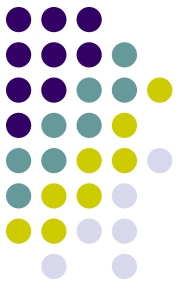


- “What authority does audit have to audit your area?”



Audit authority

- IA: Charter – Audit Committee – authority.
- Audit plan – Audit Committee sign-off.
- Audit Plan result of a consultative process. It is subject to Audit Committee approval, which then provides the organisational authority to do it.
- ANAO same – a consultative plan.
- Timing must be negotiable.
- ANAO – external imprimatur. There are more avenues to negotiate with IA.



Audit authority

- Audit should fit in with the governance framework and key timing points in SDLC and the Gateway methodology (independent assurance methodology for high risk projects.)
- Perception is that ANAO have more authority.
- Auditors should have appropriate security clearance.
- Engage with IT first, and do it early.
- IA & ANAO have same authority.
- **I've never tested it!**

CIO's & IT Managers



- “Do you know more, in general, about managing/controlling risks in your area than auditors?”

Do you know more about controlling risks than auditors?



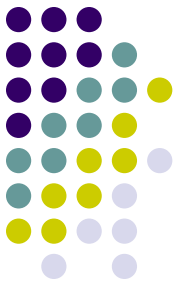
- I know more about the risks in my area, but auditors bring a focus and control framework which allows you to look at managing in a different way.
- I know more because I live the business day-to-day.
- Yes, because each agency does IT slightly differently, and the management should be across their area.
- Solutions should be client driven.
- Audits are drivers for change, and I'm happy about that!

Do you know more about controlling risks than auditors?



- Yes – I'm in the job day-in day-out to manage the business processes and risks.
- Yes, without a doubt! But there may be risks not considered that audit pick up.
- Yes, IT people are fairly formal, structured thinkers with an eye on corporate governance. But audit makes you think in a different light.
- IT tend to have different technical knowledge and skills to audit.
- Audit should work with the client to provide practical solutions.

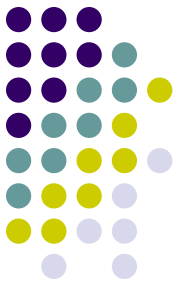
Do you know more about controlling risks than auditors?



- I don't like snotty-nosed little auditors acting like they know more than you.

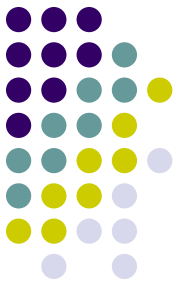
What you want is audit to help you make the project a better project.

CIO's & IT Managers



- “Must you ensure audit recommendations pertaining to your area are implemented?”

Must I implement recommendations?



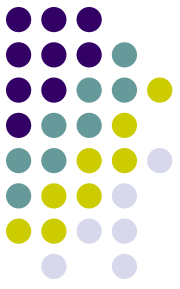
- It is very good practice to do so!
- Yes, for the ones we accept. Some we disagree with, but more common is we absolutely agree, but can't do now.
- Consultative approach: better to say gotcha, but agreed and being actioned.
- No – recommendations must be actionable, pragmatic and achievable. (i.e. budget) Should add value to the project.
- Some recommendations can't be and must be explained/ negotiated.

Must I implement recommendations?



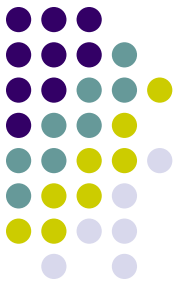
- Audit recommendations should not be ignored. But fixing requires time, money and the will.
- ANAO recommendations may escalate if not addressed.
- Issues: Timeframe, practicality, what does “implementation” mean?
- Higher risk recommendations : ANAO & Audit Committee must be satisfied.

Must I implement recommendations?



- Yes – recommendations that are logical, achievable, sensible, beneficial.
- Yes, but no surprises, please. Give an opportunity to correct errors. (Remember, build trust.)
- Generally not a problem, if the audit is well-done.
- Auditors should not give a technological answer.
- Auditors should not be alarmist, and should try to understand how the solution is being implemented.

Must I implement recommendations?

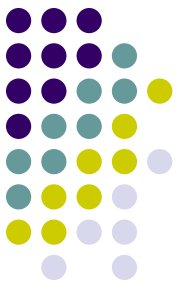


- Agree consultative solutions. (IA tend to do this).
- New auditors should try to understand: judgement vs. Fear of the unknown. (Trust).
- Get the facts right (Audit 101)! Any incorrect facts divert focus.
- Require common sense and judgement.

IT Audit – Traps for New Players



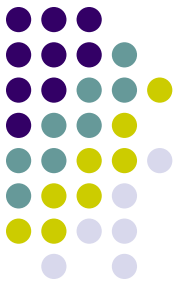
- These IT types are just trying to confuse me with jargon!



IT jargon

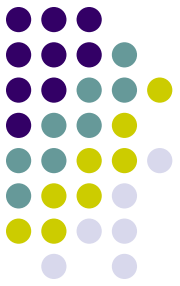
- Tech people: the lower level talk tech-talk.
- Learn a little!
- Understand the basics.
- <http://www.networkworld.com/news/2007/051607-top-10-it-jargon-slides.html?page=3>

IT jargon



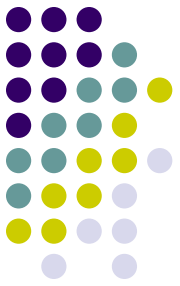
- “Your ISP should provide you with a static IP address so that they can include it in their DNS server to make sure that your website is known to the internet.”
- Translation:
Your (telecommunications) provider should provide you with a phone number (all phone numbers are unique) and also include that in the yellow pages directory to make sure that your number is known to the public.

IT jargon

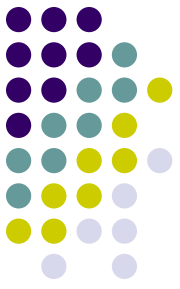


- “Yes, we are going to have to spend the night in the lab doing attack and pens, the CIO and ITSA need the results to cover off the ACSI33/ISM compliance breach.”
- Translation:
“We will need to use network attack and security penetration testing exercises to assure the Chief Information Officer and the information technology security adviser that we are complying with the Australian Government ICT Security Manual.”

IT jargon



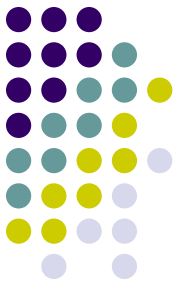
- *“and we also have a Linux box in the DMZ with Content Keeper that I use to keep tabs on the users surfing habits .”*
- Translation:
“We are monitoring users internet use.”



Conclusion

- Communicate, communicate, communicate!
- Audit and organisations should work together to achieve the best possible outcome for the organisation by open, clear communication.
- Build trust.
- Educate yourself, be informed.
- Remember: “Techo’s are sneaky and can get around anything”!
- Don’t be the snotty nosed little auditor!

Who I spoke with...



- Trevor Berryman, Chief Technical Officer, Geoscience Australia
- John Trabinger, Branch Manager CBMS Redevelopment Project, Dept of Finance & Deregulation
- Ken Pettifer, Division Head Innovation and formerly CIO, Dept of Innovation, Industry, Science & Research
- Greg Farr, CIO, Dept of Defence
- Eija Seittenranta, General Manager Business Systems, Centrelink
- Peter Alexander, Branch Manager On-Line Services, Australian Government Information Management Office (AGIMO)
- Steve Dodt, Manager ICT Department of Resources, Energy & Tourism