Information Commissioner's Office

Good Practice Department

Victoria Heath

2 April 2014

ico.
Information Commissioner's Office

What is good practice?

- What the DPA says?
  - Good practice is defined as such practice for processing personal data as appears to be desirable. Includes, but is not limited to, compliance with the requirements of the act
- What does this mean in practice?
  - Efficient, effective, robust policies and procedures exist and are working in practice to ensure information is handled correctly and the organisation is aware of, and fulfilling, its obligations

Good practice audit programme

- Seen as being key to educating and assisting organisations to meet their obligations
- Risk based focussed on ICO areas of priority - audits are targeted to where research and ICO business intelligence identifies organisations that may benefit most from our assistance
- Use audit, assessment and practical advice and recommendations to improve the way organisations deal with information rights issues
- Assist the ICO to share knowledge and promote good data protection practice through publishing audit outcomes
- Allow organisations to show their commitment to, and recognition of, the importance of data protection

ico.
Information Commissioner's Office

Audits: consensual and compulsory

- So far, all of our audits have been consensual – i.e. scope and time agreed with the data controller or point of contact
- Consensual audits extend to the following of good practice – including the Act, codes of practice and guidance
- Now have powers to conduct ‘compulsory’ audits following the issue of an Assessment Notice (section 41A of DPA).
- For this we have developed a Code of Practice
- Strategy is to actively seek consensual audits wherever possible

ico.
Information Commissioner's Office

Audits & Enforcement

- Not intended that audits will lead to formal enforcement action – seen as a way of encouraging compliance and good practice
- The Information Commissioner will **not** impose a monetary penalty as a result of non-compliance discovered in the course of an audit
- However, where a breach occurs, ICO guidance on monetary penalties considers refusal of an audit which could reasonably have been expected to reveal relevant risks to be an aggravating factor
- Also, reserve the right to use powers in case of any identified major non-compliance where the data controller refuses to address a recommendation within an acceptable timescale
- Note: failure to comply with the terms of an assessment notice will be grounds for a judge to issue a warrant for entry and inspection under Schedule 9 of the Act

ico.
Information Commissioner's Office

Tasking & Co-ordinating

- Monthly meeting with Enforcement (pre project Eagle)
- Monthly meeting of Operations with Policy Delivery and Strategic Liaison (project Eagle)
- Discuss serious concerns about organisation's information rights practice
- Sector specific
- Decide actions to be taken

ico.
Information Commissioner's Office

Advisory visits

- Launched December 2011 – over 700 volunteers to date
- Aimed at small to medium sized organisations
- 1 day short, informal advisory visit, 1 person
- Short report provided within one week and outcome reports for sectors, e.g. charities, community organisations
- Make more effective use of Good Practice resource

ico.
Information Commissioner's Office

Workshops

- Piloted during 2013 and aimed at small to medium sized organisations and targeted at non specialists
- Free 1 day short interactive format 15-40 attendees
- Opportunity to work alongside experienced ICO staff
- Resources to be made available
- Summary of resources and guidance referenced

Information Risk Reviews

- Less formal than audit, more formal than AV
- Specific scope informed by referral from T & C
- 1 person, maximum 2 days
- Report highlighting recommendations on priority basis

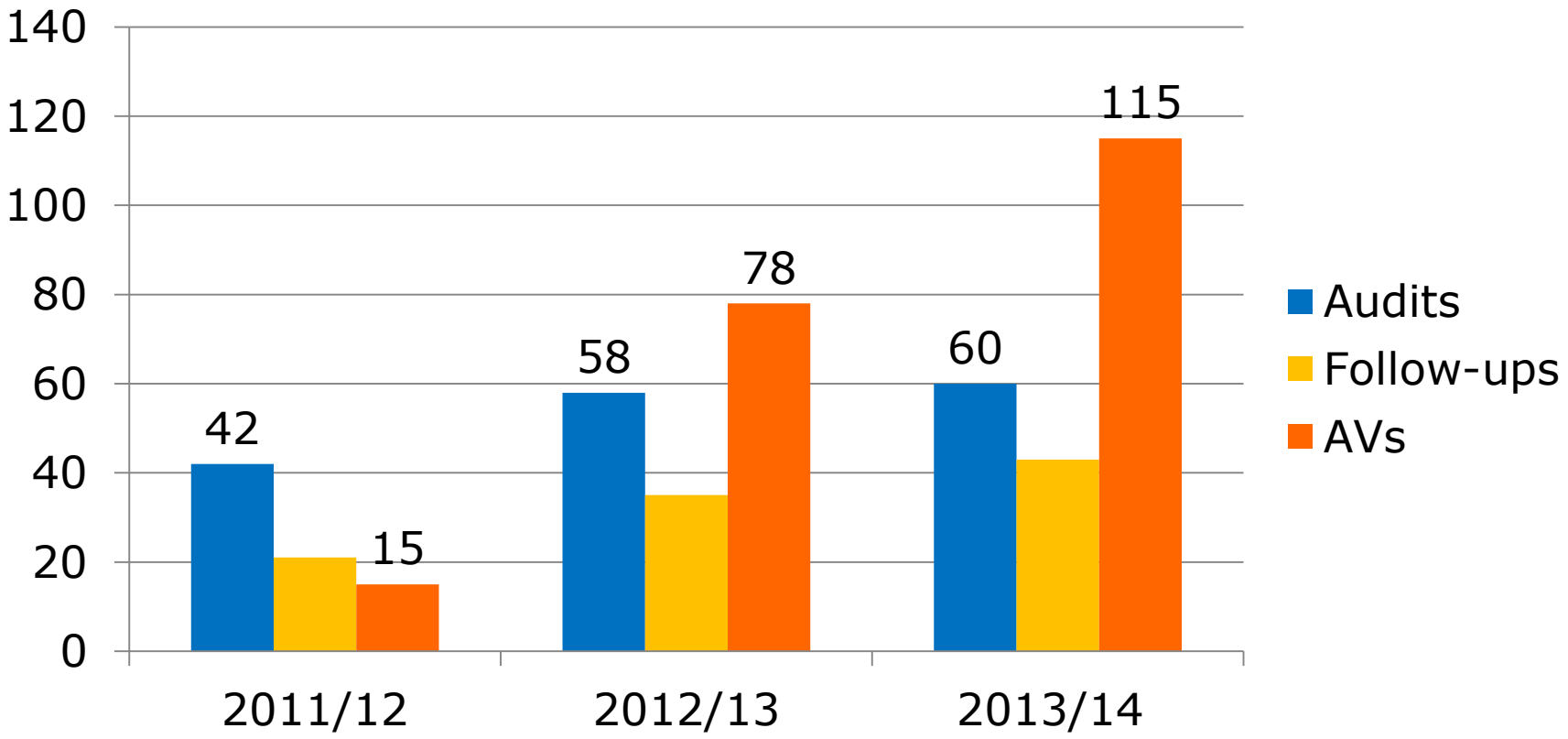
ico.
Information Commissioner's Office

Self Assessment

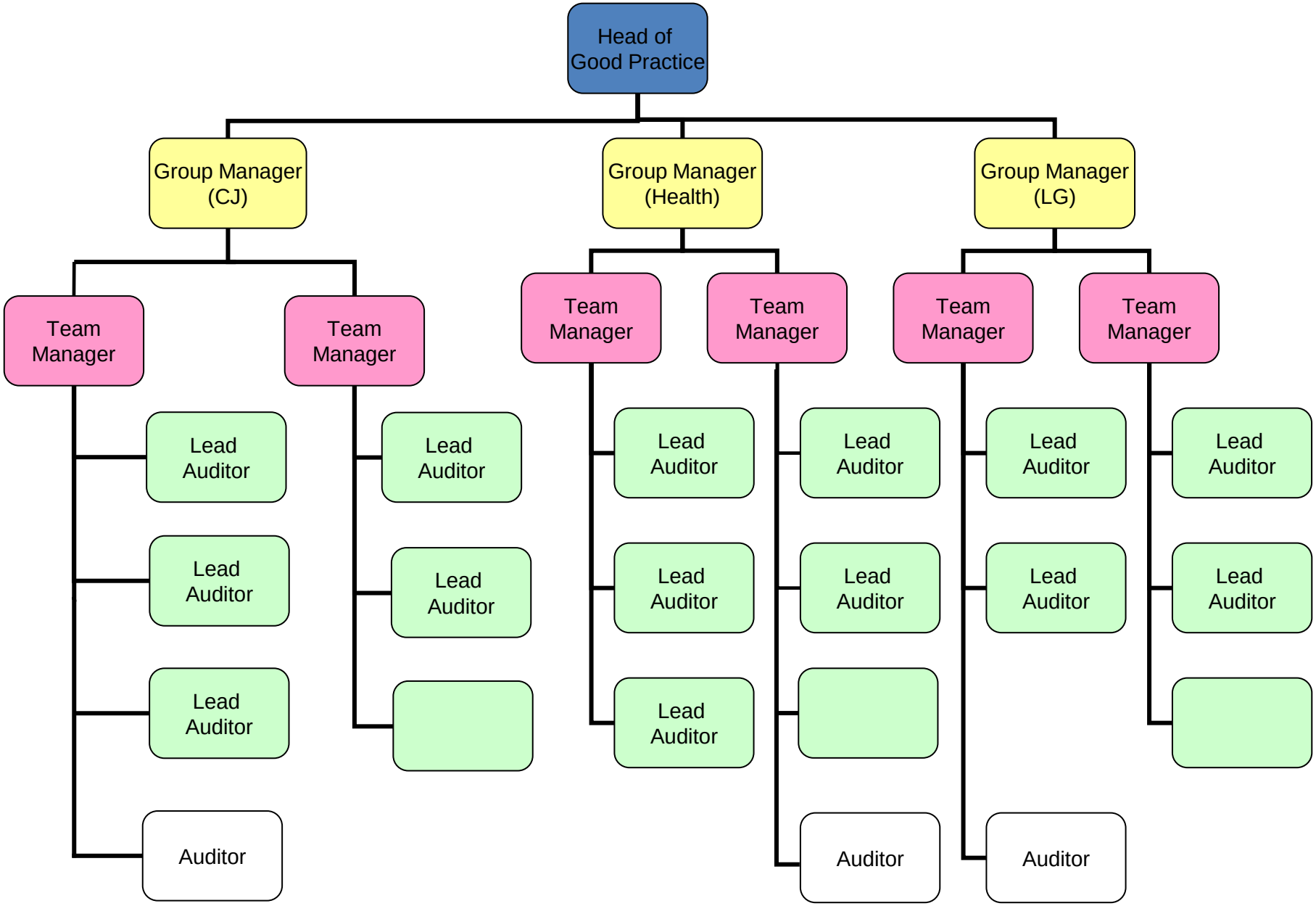
- Project to produce online tools to allow data controllers to assess their own data protection compliance
- No direct ICO involvement
- Local authority (governance scope) developed and currently being tested
- SME version – first prototype being produced

ico.
Information Commissioner's Office

Audits, follow-ups & AVs completed



ico.
Information Commissioner's Office


Head of Good Practice
Group Manager (CJ)
Group Manager (Health)
Group Manager (LG)
Team Manager
Team Manager
Team Manager
Team Manager
Team Manager
Team Manager
Lead Auditor
Lead Auditor
Lead Auditor
Auditor
Lead Auditor
Lead Auditor
Lead Auditor
Lead Auditor
Lead Auditor
Lead Auditor
Lead Auditor
Lead Auditor
Auditor
Lead Auditor
Lead Auditor
Auditor
Lead Auditor
Lead Auditor
Auditor