Auditing cyber security

Gemma Diamond

Senior Manager

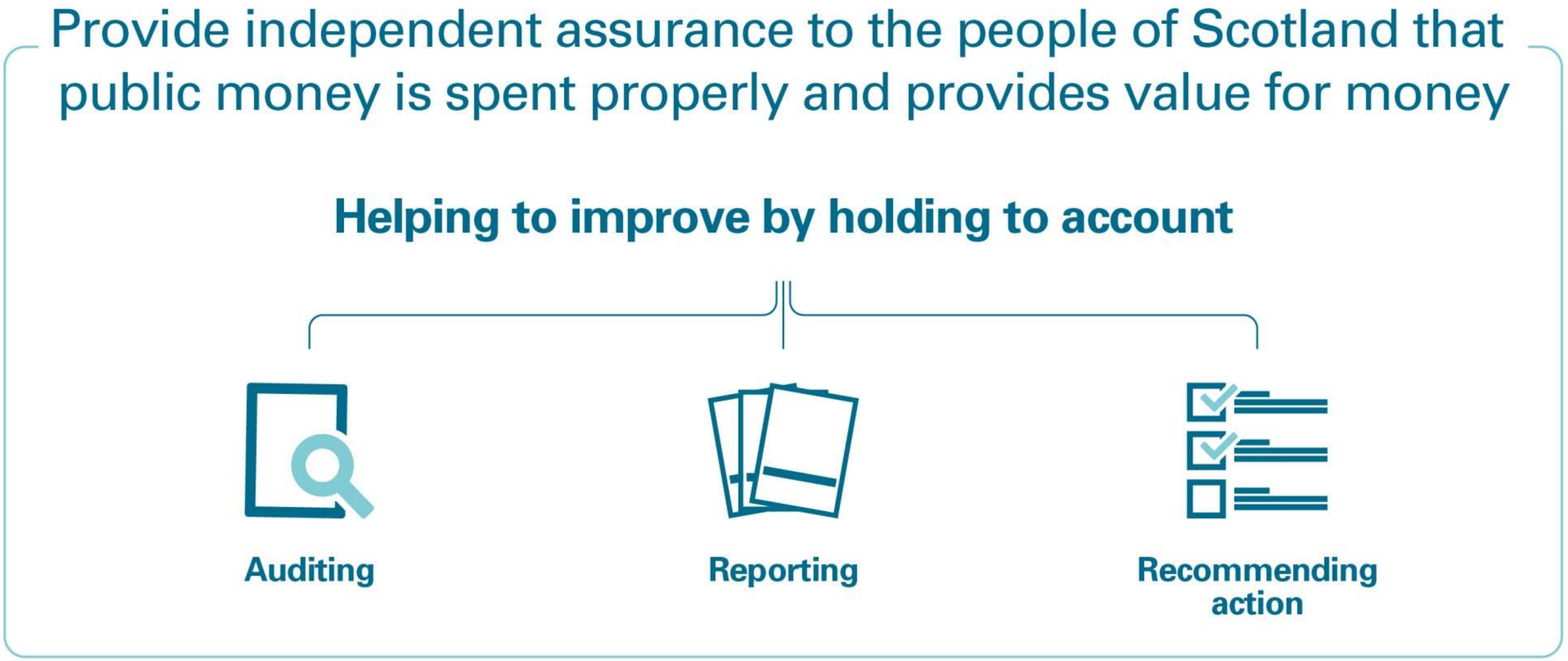
AUDIT SCOTLAND

Public Audit in Scotland

77	Central government bodies and Scottish Parliament (including police, fire, Scottish Water)
23	NHS bodies
32	Councils
73	Joint boards and committees (including 30 health integration boards)
21	Further education colleges

226 Public bodies audited

Audit Scotland – role



Provide independent assurance to the people of Scotland that public money is spent properly and provides value for money

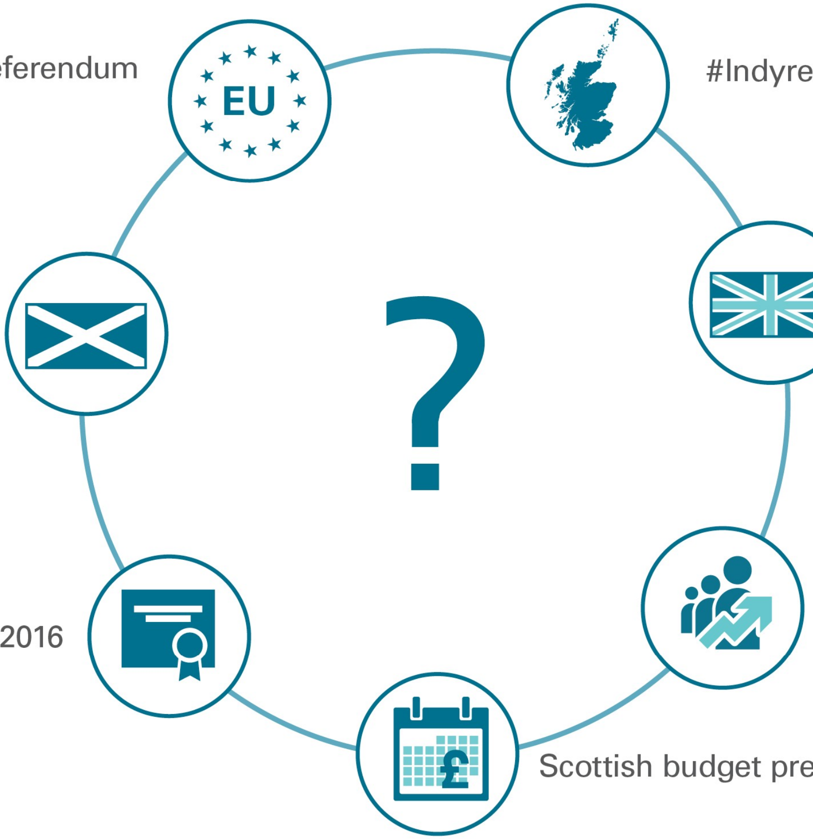
Helping to improve by holding to account

Auditing

Reporting

Recommending action

Key issues for Audit Scotland



EU referendum

#Indyref2

New Scottish Parliament

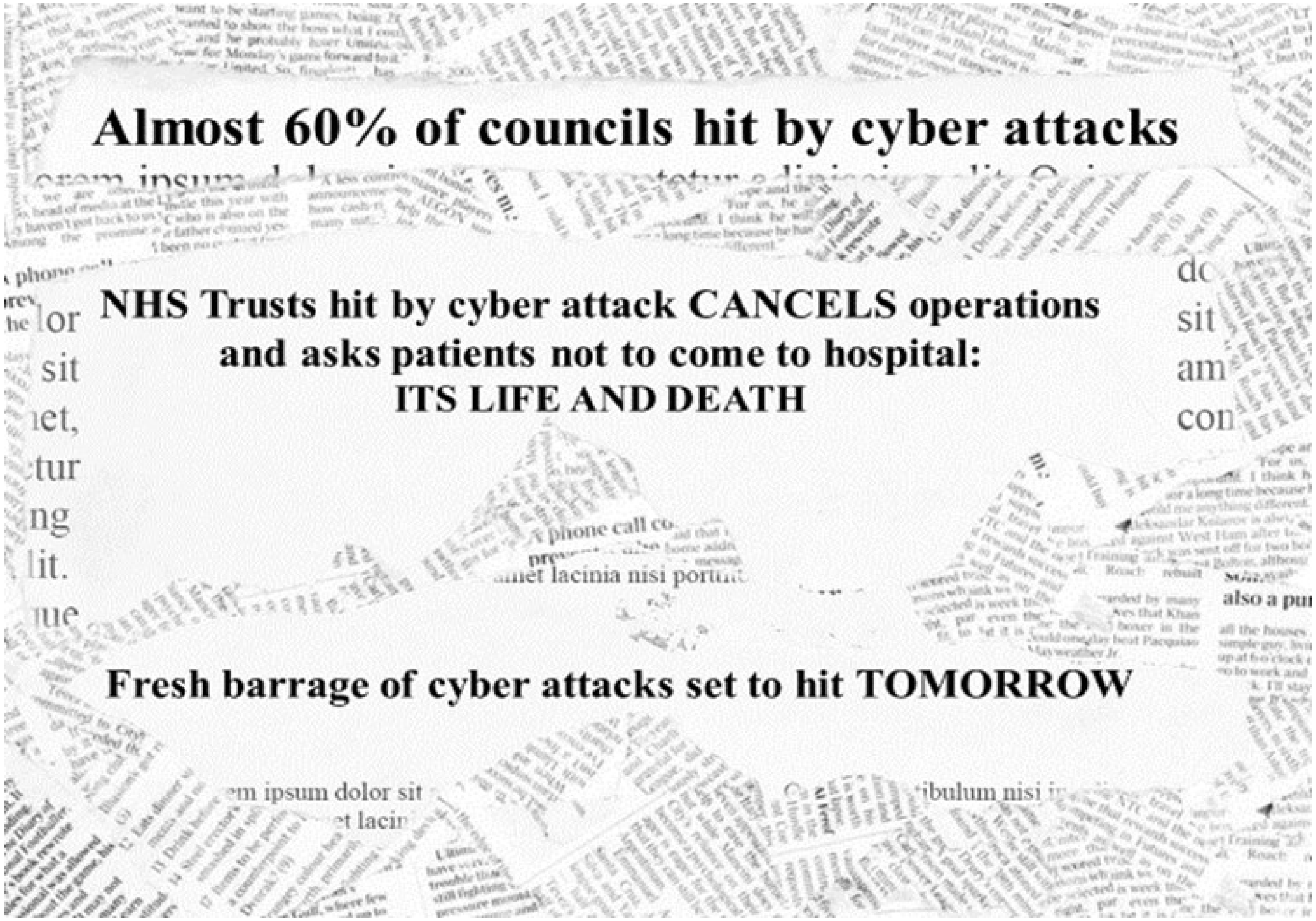
New UK Government

Scotland Act 2016

Ageing population

Scottish budget pressures

Cyber headlines



Almost 60% of councils hit by cyber attacks

NHS Trusts hit by cyber attack CANCELS operations and asks patients not to come to hospital: ITS LIFE AND DEATH

Fresh barrage of cyber attacks set to hit TOMORROW

Risk identification

Discussions with stakeholders

Consistent news coverage

Parliamentary interest and questions

New powers for Scottish Government

Impact of cyber attacks for citizens

= Audit risk

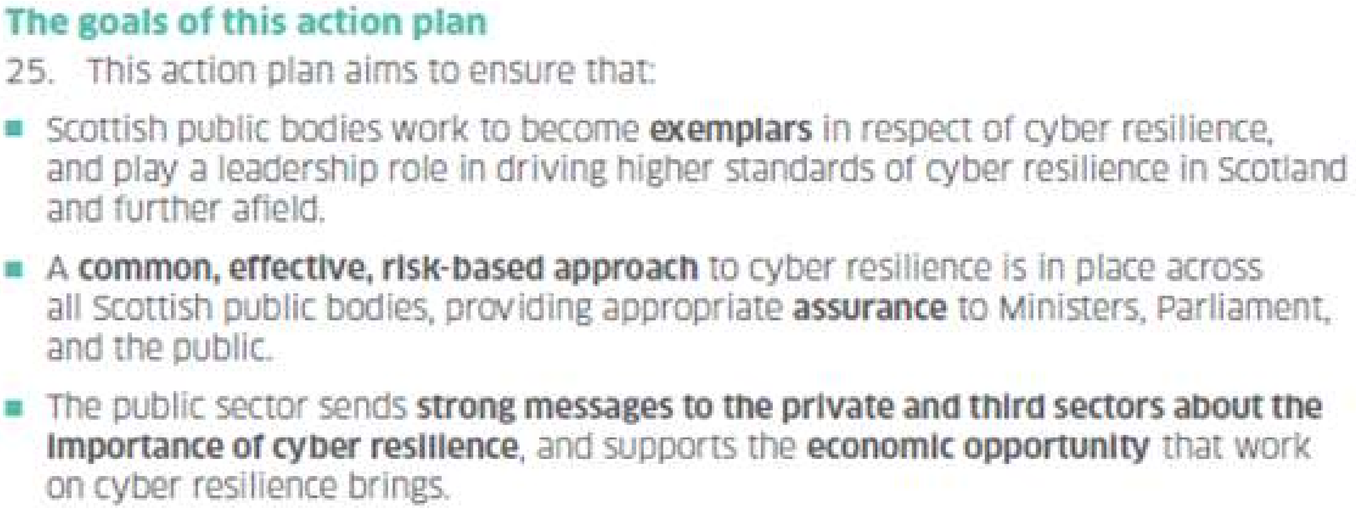
Scottish Government action

www.gov.scot/cyberresilience

Scottish Government
Riaghaltas na h-Alba
gov.scot

SAFE, SECURE AND PROSPEROUS:
A CYBER RESILIENCE STRATEGY FOR SCOTLAND

PUBLIC SECTOR ACTION PLAN 2017-18



The goals of this action plan

25. This action plan aims to ensure that:

- Scottish public bodies work to become **exemplars** in respect of cyber resilience, and play a leadership role in driving higher standards of cyber resilience in Scotland and further afield.
- A **common, effective, risk-based approach** to cyber resilience is in place across all Scottish public bodies, providing appropriate **assurance** to Ministers, Parliament, and the public.
- The public sector sends **strong messages to the private and third sectors about the importance of cyber resilience**, and supports the **economic opportunity** that work on cyber resilience brings.

Our audit work

Guidance for auditors:

> *"It has been developed to help auditors assess how public bodies are considering cyber security risks, and the appropriateness of risk management and governance arrangements for cyber security."*

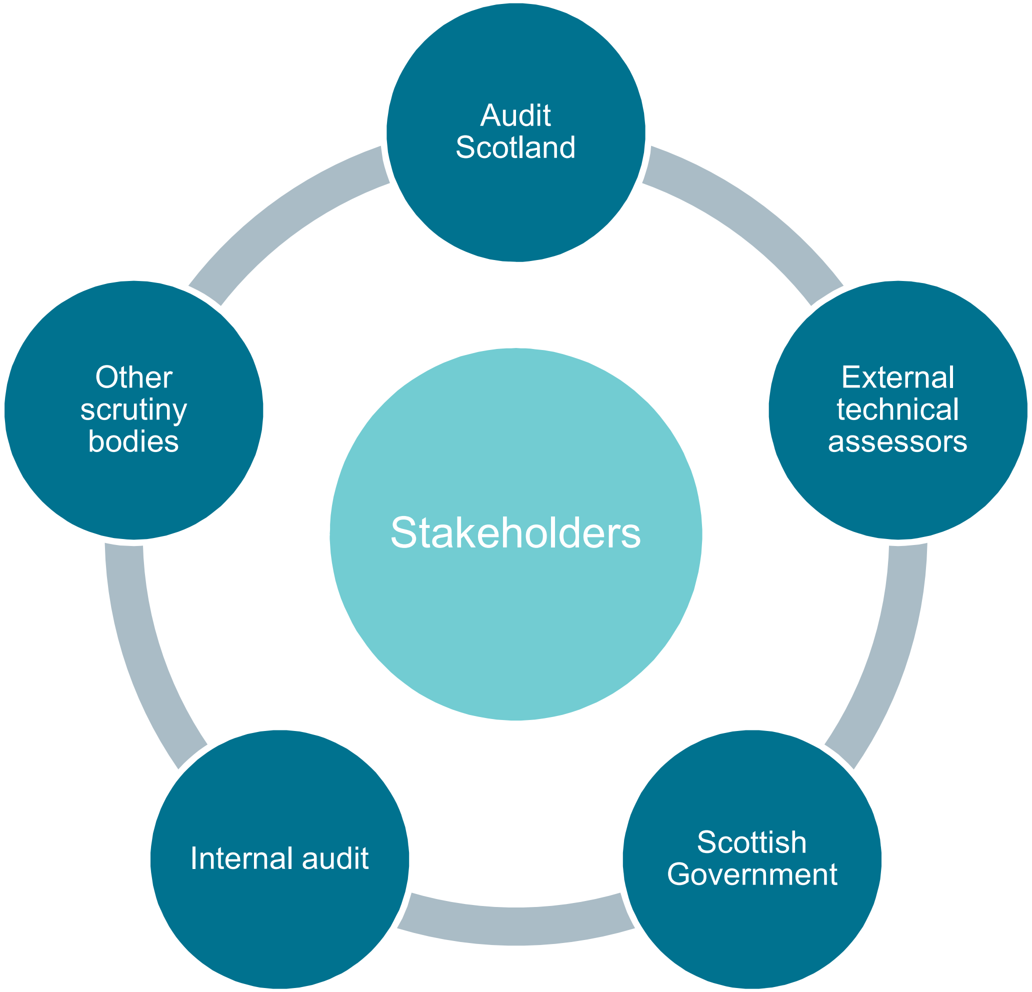
- Three high-level prompts
  - Does the public body have a structured approach to cyber security which guides its activity and expenditure?
  - How has management decided what risk it will tolerate and how does it manage that risk?
  - Has the public body identified and deployed the capability it needs?

Our audit work

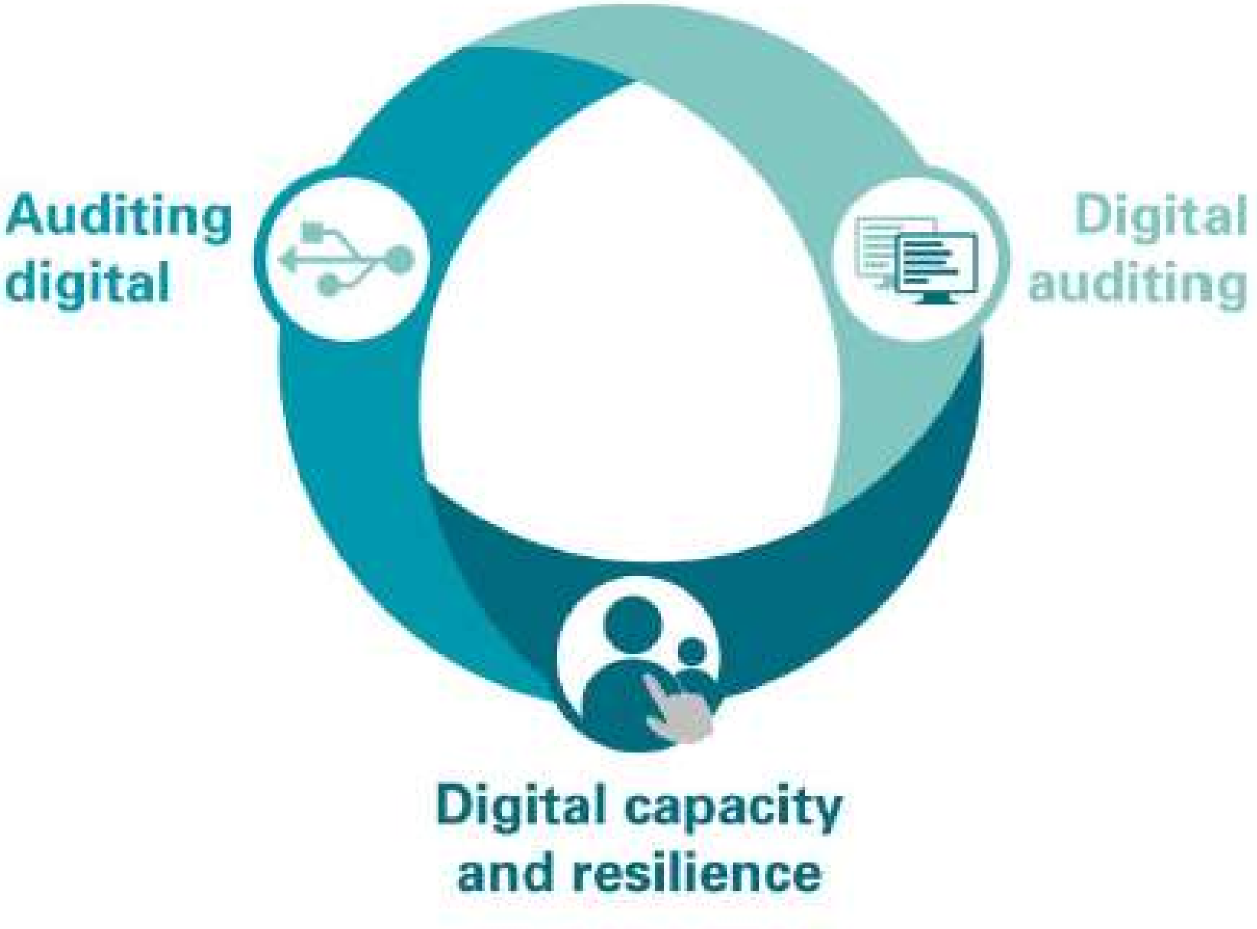
Importance of culture and behaviours:

> *“While auditors should look at the processes and procedures in place, they should also consider the culture and behaviours within the organisation. In the Scottish Government guidance the National Cyber Resilience Leaders Board emphasises that **cyber resilience is as much a cultural issue as a technical one**. They view it as vital that Scotland's public bodies understand and manage the cyber threat at Board/Senior management level, and take action to **promote a culture of cyber security** and awareness at all levels of the organisation.”*

Working with others



Our skills and capacity



Discussion and further information

https://www.facebook.com/pages/Audit-Scotland/1649085352037675

https://twitter.com/auditscotland

www.audit-scotland.gov.uk/newsletter