Incident Response and Investigations

Regulation and standards

n-gate ltd.

http://www.n-gate.net/

2 related activities

- Forensic Science Regulation
- ISO/IEC JTC1 SC27 work on IS Incident Investigations

Background

- Forensic Science on Trial
- Omagh Judgment
- Strengthening Forensic Science in the United States : a path forward

Background

- Common themes
  - scrutiny of methods
  - proof of fitness for purpose
  - qualification of “experts”
  - comparability & compatibility

Forensic Science Regulation

- EU push to harmonise evidential standards
  - reducing cross-border problems
  - UK concerns about deployment of new methods without sufficient testing
    - e.g. low template DNA in the Omagh bombing case

Forensic Science Regulator

- Andrew Rennison
- Appointed in 2008 to advise on quality for Forensic Science Providers providing evidence into the Criminal Justice System
  - i.e. ALL prosecution expert/scientific witnesses
- Codes of Conduct & Practice published in 2010
  - Compliance by 2013 (2015 for Digital Evidence)
  - Digital Evidence was the first area addressed

Regulator's Codes

- build on ISO/IEC 17025 (laboratory based) and ISO/IEC 17020 (crime scene)
- combined with ILAC-G19

December 2011

European Council document 17537/11

"*Draft Council Conclusions on the vision for European Forensic Science 2020 including the creation of a European Forensic Science Area and the development of forensic science infrastructure in Europe*"

n-gate ltd.

http://www.n-gate.net/

"CONSIDERING Council Framework Decision 2009/905/JHA on Accreditation of forensic service providers carrying out laboratory activities, which seeks to ensure that the results of laboratory activities carried out by accredited forensic service providers in one Member State are recognised by the authorities responsible for the prevention, detection and investigation of criminal offences as being equally reliable as the results of laboratory activities carried out by forensic service providers accredited to ***EN ISO/IEC 17025*** within any other Member State, and to achieve this by ensuring that forensic service providers carrying out laboratory activities are accredited by a national accreditation body as complying with ***EN ISO/IEC 17025***,"

"EMPHASISING therefore the need to define commonly accepted minimum forensic science standards for the collection, processing, use and delivery of forensic data relating inter alia to data concerning DNA profiles, as well as dactyloscopic and other biometric data, and ***to equip the Union to meet the new challenges that it is facing in the field of high tech and cyber crime***,"

"INVITES THE MEMBER STATES AND THE COMMISSION, in close cooperation with Europol, ENFSI and other such international organisations as Member States consider appropriate to present ***by the end of June 2013*** a detailed action plan to implement the vision for European Forensic Science 2020 set out in annex , taking into account the final project report "*Safeguarding the use of expert evidence in the European Union" (JLS/2006/AGIS/058)*, the final project report "*Study of the obstacles to cooperation and information-sharing between forensic science laboratories and other relevant bodies of different Member States and between the latter and counterparts in third countries" (JLS/D1/2007/025)*, and the Green Paper on obtaining evidence in criminal matters from one Member State to another and securing its admissibility *(17691/09 COPEN 249 JAI 935)*,"

ISO17025 - 3 pillars

- Competence - staff
- Validation - method
- Proficiency - process

n-gate ltd.

http://www.n-gate.net/

Meanwhile...

n-gate ltd.

http://www.n-gate.net/

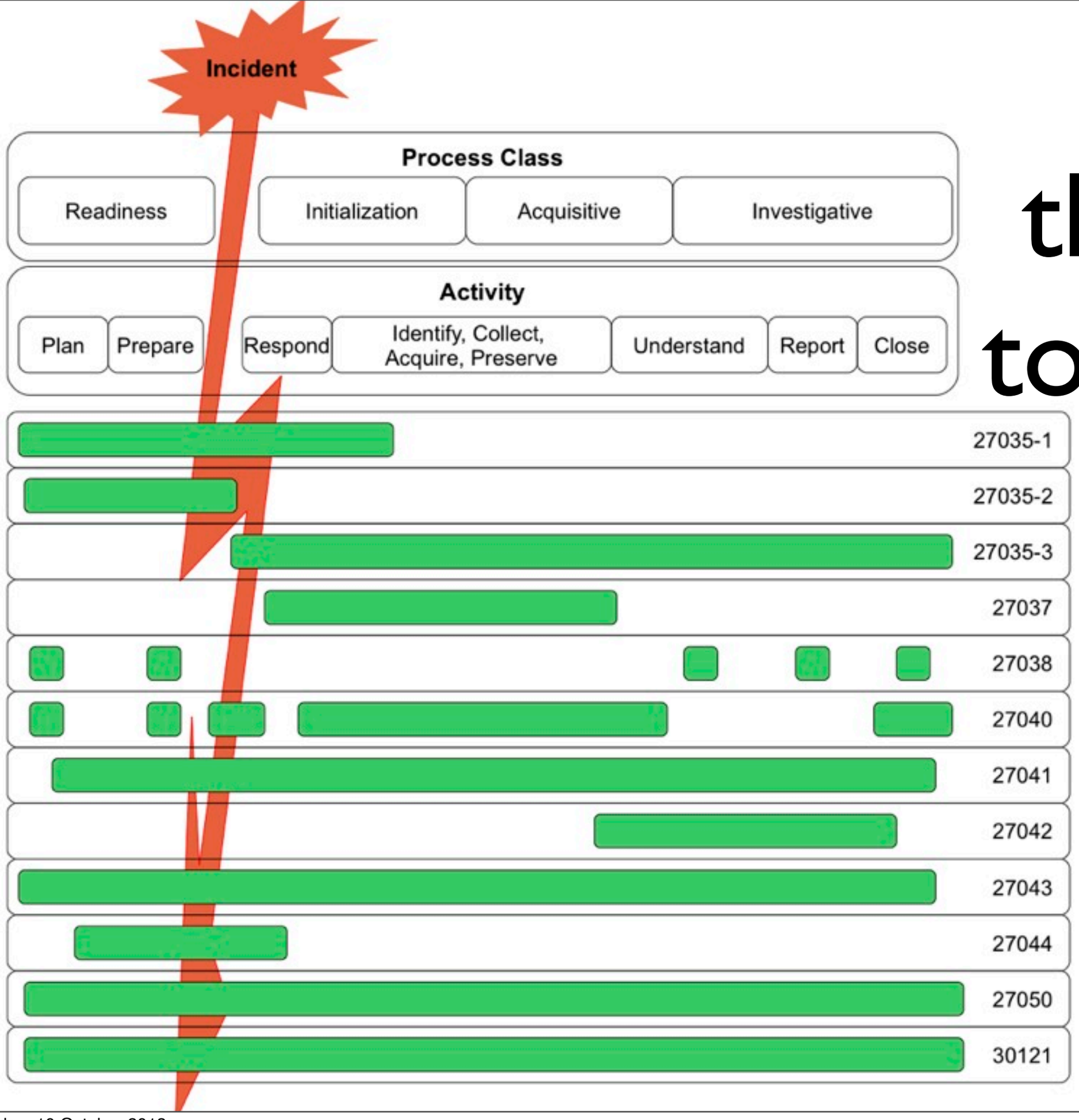
Parallel work : ISO

- ISO/IEC JTC1 SC27 WG4 (Information Security)
  - working on ISO/IEC 27037 since 2009
  - Published November 2012
  - “Guidelines for the Identification,collection, acquisition and preservation of digital evidence”
    - a “first responder” guide to the point of imaging
    - includes CCTV

Near-completion ISO projects

- Investigation Principles & Processes (27043)
- Guidelines for Analysis & Interpretation of Digital Evidence (27042)
  - These will have similar requirements to 27037
- Guidance on assuring suitability and adequacy of investigation methods (27041)
  - will define validation in particular - may address competence & proficiency if required

How they fit together



Key

- 27035 - Incident Response, including investigative readiness
- 27037 - First investigative response
- 27042 - Conducting the investigation
- 27041 - assuring investigations are correct
- 27043 - Investigative models and principles
- 27040 - storage security
- 27038 - redaction
- 27044 - Security Incident Event Management (SIEM)
- 27050 - eDiscovery (*NEW!*)
- 30121 - “forensic” governance

Common themes

- In the regulatory framework and the ISO/ IEC standards
  - ISO 900x type quality system

PLUS

- Evidence of staff competence
- Evidence of organisational proficiency
- Evidence that methods are fit for purpose

Effect

- Lots of time & effort spent getting things right
- Reduction in number of cases lost because of mistakes at the start
    - e.g. failing to establish continuity of evidence, or application of incorrect processing leading to tainted evidence
- Reduction in time spent on unnecessary or pointless activity

More information ?

Angus Marshall

(UK principal expert on digital evidence to ISO and editor/co-editor of 27041, 27042 and 27050)

angus@n-gate.net

n-gate ltd.

http://www.n-gate.net/