



A&L Goodbody

Managing Investigations – Technological Benefits & Risks

Kate Harnett, White Collar Crime Associate

11 December 2020

“The temptation to form premature theories upon insufficient data is the bane of our profession.”

— Arthur Conan Doyle, Sherlock Holmes, The Valley of Fear

Discussion Points



Economic Crime Enforcement Landscape

- Increasing focus on corporate offending
- Reporting Obligations
- Recent Developments
- Hamilton Report's Recommendations



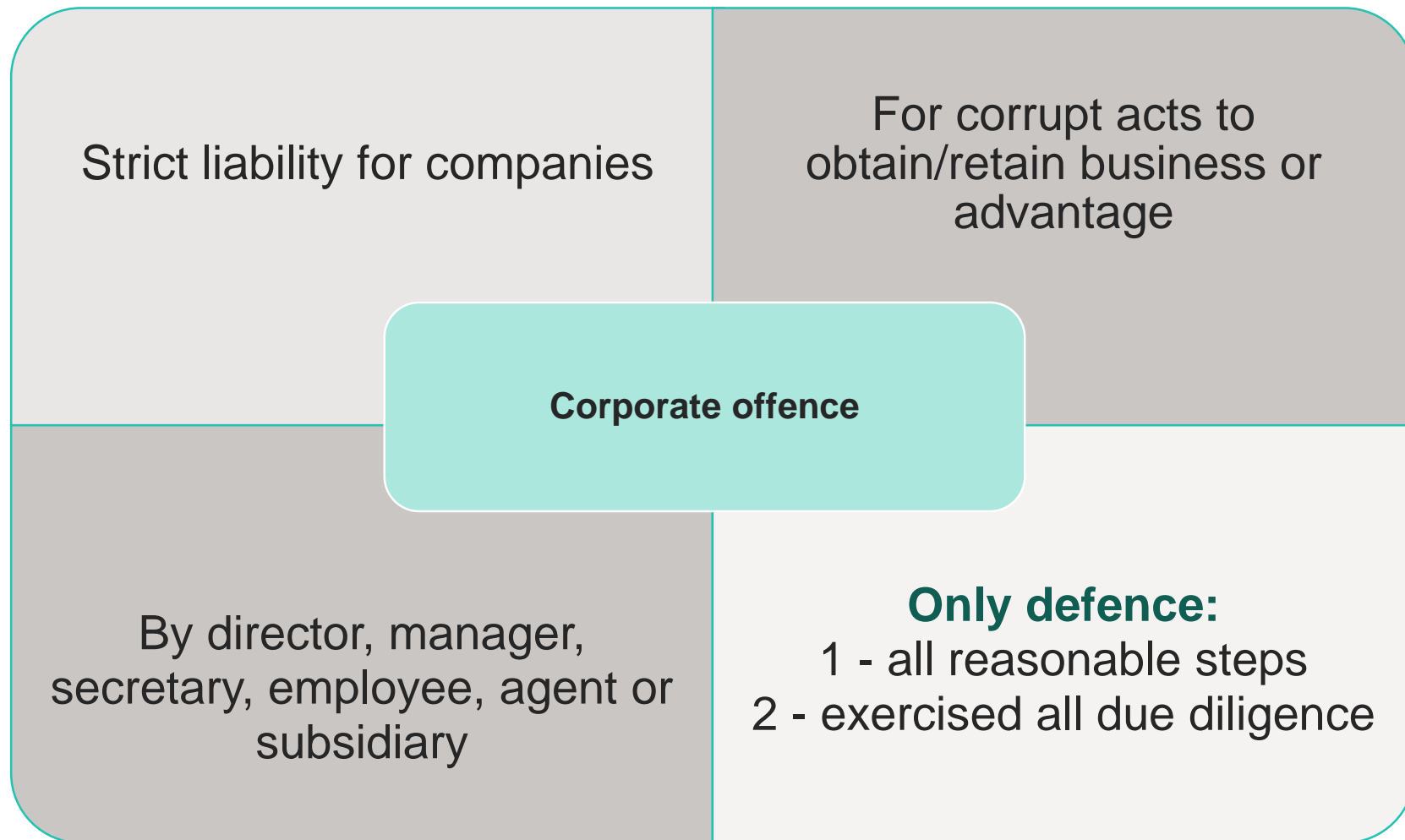
Corporate Investigations

- Technology in Internal investigations: Benefits v. Risks
 - Gathering Evidence - Digital Data
 - Interviews
 - Remote Investigations
- Digital Data Challenges for State Investigators




Irish Corporate Enforcement Landscape



Corruption - Corporate Offence - S.18 CJ(CO)A 2018



Corruption - Cross-jurisdictional comparison

	Ireland  Criminal (Corruption Act 2018) Justice Offences)	UK  Bribery Act 2010	USA  Foreign Corrupt Practices Act 1977
Does the legislation criminalise both public and private sector corrupt acts?	Yes	Yes	No – Public Sector Only
Does the legislation have extra-territorial effect?	Yes	Yes	Yes
Is it an offence to accept / request / agree to receive a corrupt payment?	Yes	Yes	No
Is mandatory reporting required to the authorities for relevant offences?	Yes	No	No
Does the legislation include a “failure to prevent” offence for corporates?	Yes	Yes	No
Is a business expenses exception available?	No	No	Yes
Is a facilitation payments exception available?	No	No	Yes

Personal Liability for Senior Company Officers

- Section 18(3) CJ(CO)A 2018
- Applies to **directors, managers, secretaries or other officers** of a company
- These individuals will be personally liable for a corruption offence committed by the company where it was committed with their **consent or connivance or was attributable to any wilful neglect** on their part.
- Supreme Court decision 28th May 2020 – **DPP v TN**
- See also **Senior Executive Accountability Regime (SEAR)**



Potential Reporting Obligations

Section 19 of the Criminal Justice Act 2011 (Withholding Information)

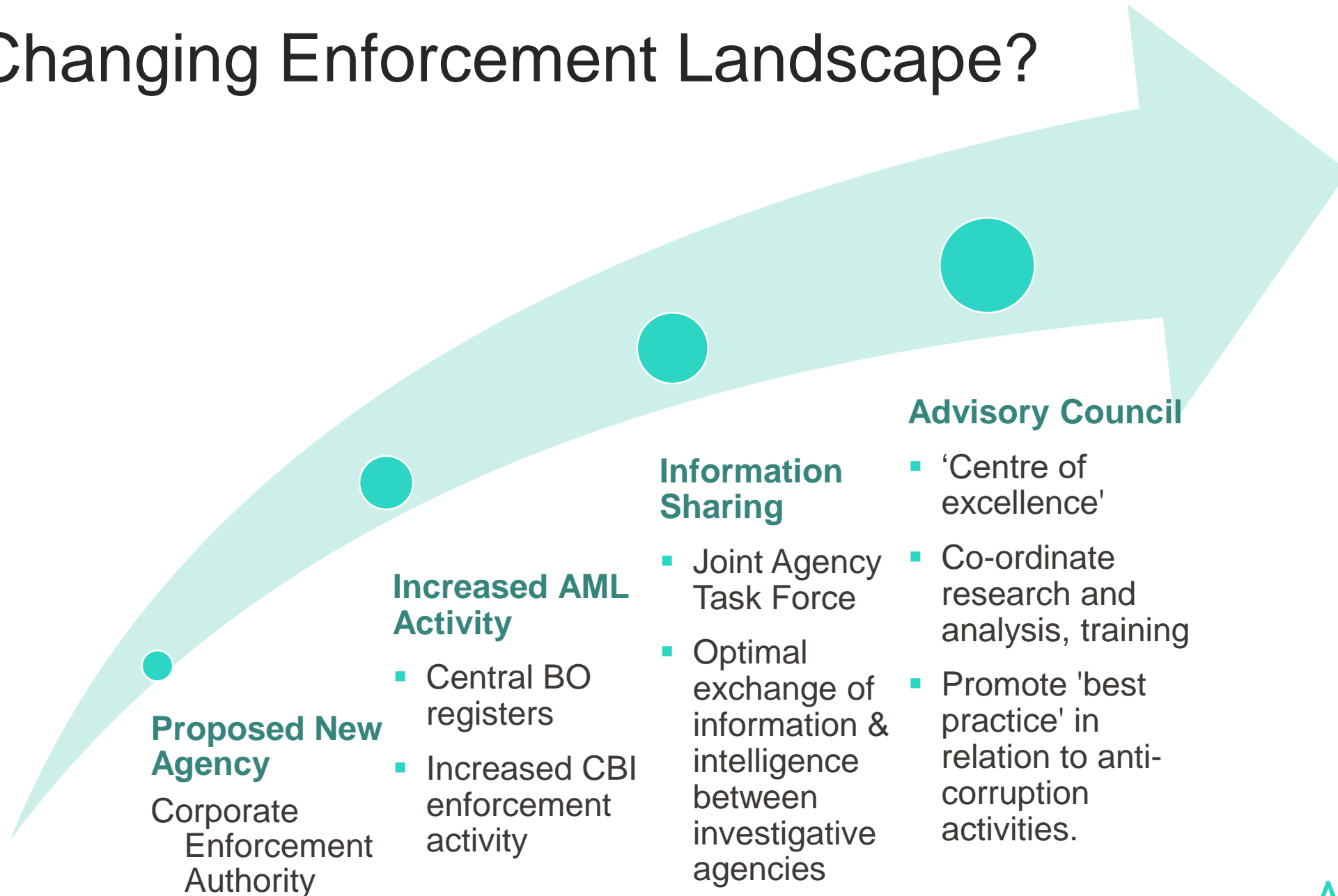
Section 59 of the Criminal Justice (Theft and Fraud Offences) Act 2001 (Reporting of offences)

Section 42 of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (Requirement for designated persons and related persons to report suspicious transactions)

Section 392 of the Companies Act 2014 (Report to Registrar and to Director: accounting records)

Section 393 of the Companies Act 2014 (Report to Registrar and Director: category 1 and 2 offences)

A Changing Enforcement Landscape?



Hamilton Review Group Report

25 Key
Recommendations

- Reviewed “***structures and Strategies to Prevent, Investigate and Penalise Economic Crime and Corruption***”, published 3 December 2020
- Highlighted need for a **more integrated approach** between State bodies, **increased resources**, and **adequate expertise** to investigate alleged offences.
- Firm recommendation that the **creation of a single standalone agency** to deal with all issues relating to the prevention, investigation and prosecution of corruption is **not required**.

Department of Justice: *"implementing new anti-fraud and anti-corruption structures informed by the work of the Review Group is a Programme for Government commitment and Minister McEntee **has received cabinet approval to bring forward an implementation action plan for the Report's recommendations**. This will include set timelines for the introduction of a series of reforms to strengthen the State's capacity to prevent and prosecute white-collar crime".*

What sparks a “corporate investigation”?

“CBI launches review of mortgage tracker scandal”

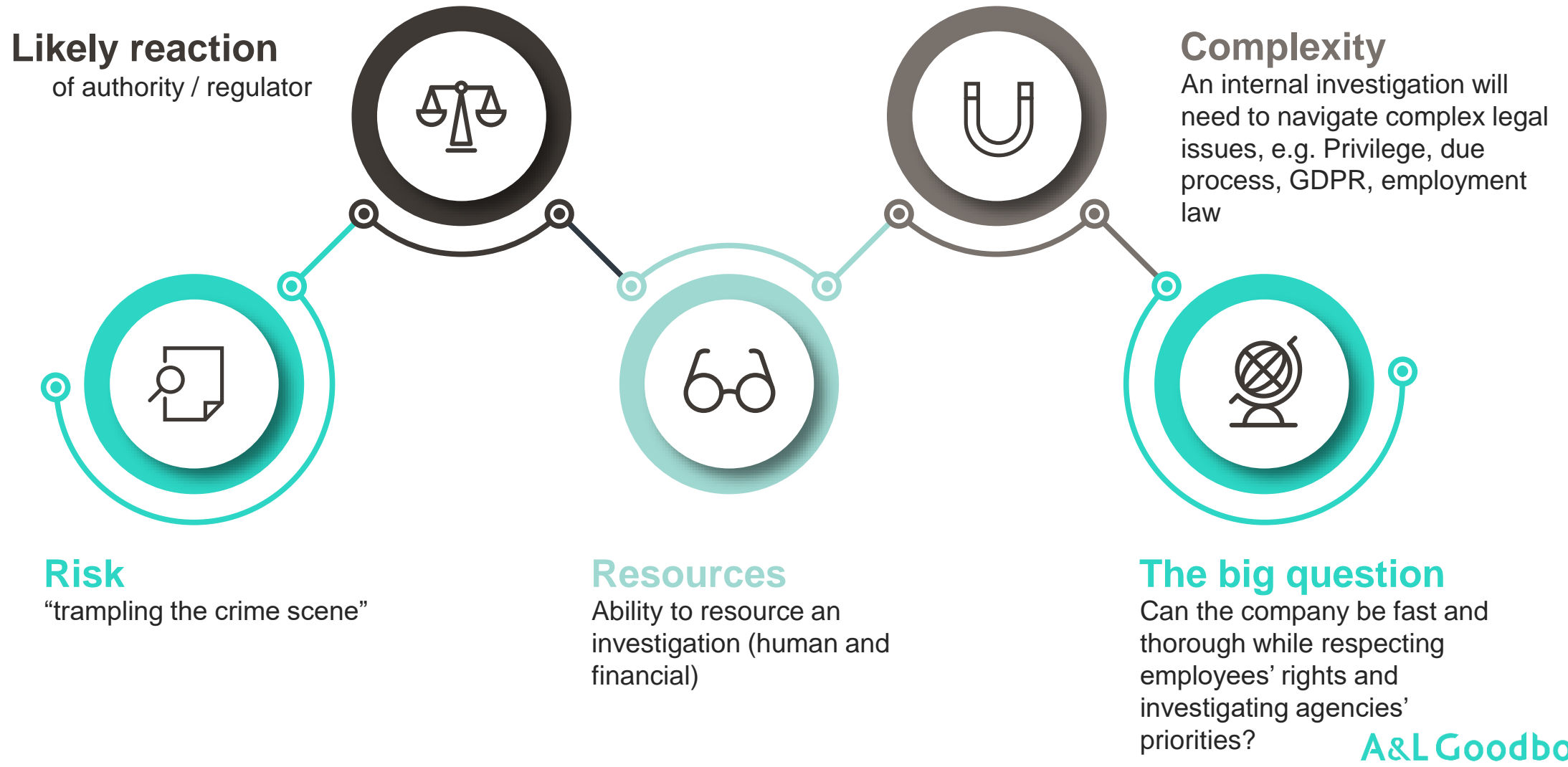
Volkswagen Headquarters Raided Again Over Diesel Scandal

“Whistleblower alleges senior manager accepted bribes”

“Customer complaints land insurance company in hot water with regulator”

Employee engaged in campaign of harassment.

Internal Company Investigations



Data Reviews & Analysis

- Exponential growth in volumes of data.
- Technology-assisted review ("TAR") – algorithm-based method of reviewing documents for relevance.
- Sensible and cost-effective way to handle large-scale reviews and productions.

Regulatory Investigations

Internal investigations /
Fact Finding

Data Subject Access
Requests

Freedom of Information
Requests

ALG DPG

Analyze

Analyze data and review output with bespoke and customizable workflows, designed by lawyers.

Review

Review documents in the most cost effective and efficient way.

Process

Provide initial data culling, de-duplication and email threading of large datasets.

Systems

Work with clients to create systems and processes to enable coordinated data collection and analysis in the event it is required

Advise

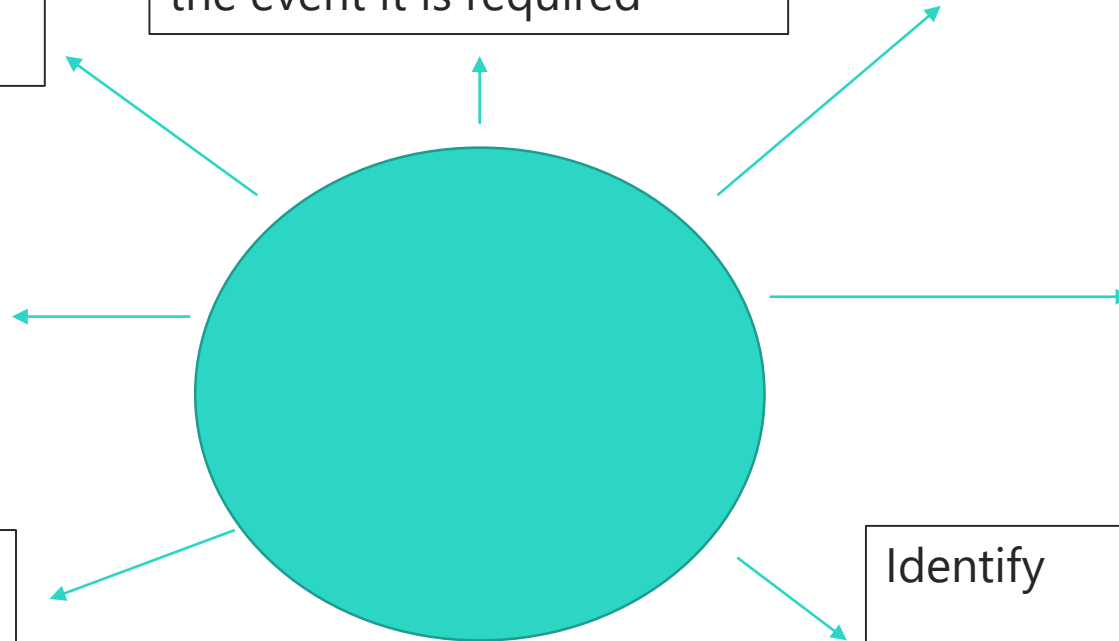
Advise clients on complying with their legal obligations at every step of a project.

Preserve

Ensure clients comply with their obligations to preserve data in line with best legal practice.

Identify

Assist clients with locating potentially relevant data.



TAR - Court Approval

IBRC & Ors. v. Sean Quinn & Ors. [2015]

Irish Court **endorsed the use of TAR** and **predictive coding methods** to assist the Irish Bank Resolution Corporation to review some 680,000 documents - (reduced from an initial 1.7 million through the use of search terms filters)

The Court noted that no method of review was 100% accurate but that even if it were only as accurate as a manual review, **TAR would still be quicker and cheaper** than manual review.

The Court held that any TAR process **must include checks and balances** which rendered each stage capable of **independent verification**.

Digital Technology: Gathering the Evidence

- **Wealth of potential information / evidence:**

- **(Double Edged Sword)**

- > Devices - mobile phones / computers / tablets / external hard drives
- > Information - emails / text messages / instant and other forms of electronic correspondence/ internet history / deleted files

- **Challenges in obtaining evidence:**

- > Passwords
- > Information on Personal Devices / Social Media Accounts
- > Encryption
- > Deletion of Data
- > Privacy Rights
- > Data Protection Rights

Necessity to Manage Data

Communication
With key individuals.
Significant adverse
consequences if
documents are
missing or destroyed
once company is on
notice

Hold Notices
to secure all relevant
soft and hard copy
documents

01



02



03

IT Department

Should be briefed on
requirements,
including suspension
of routine document
destruction exercises

04

GDPR

protocols and
permissions must be
straight before
beginning to review
emails/texts.



Document requests

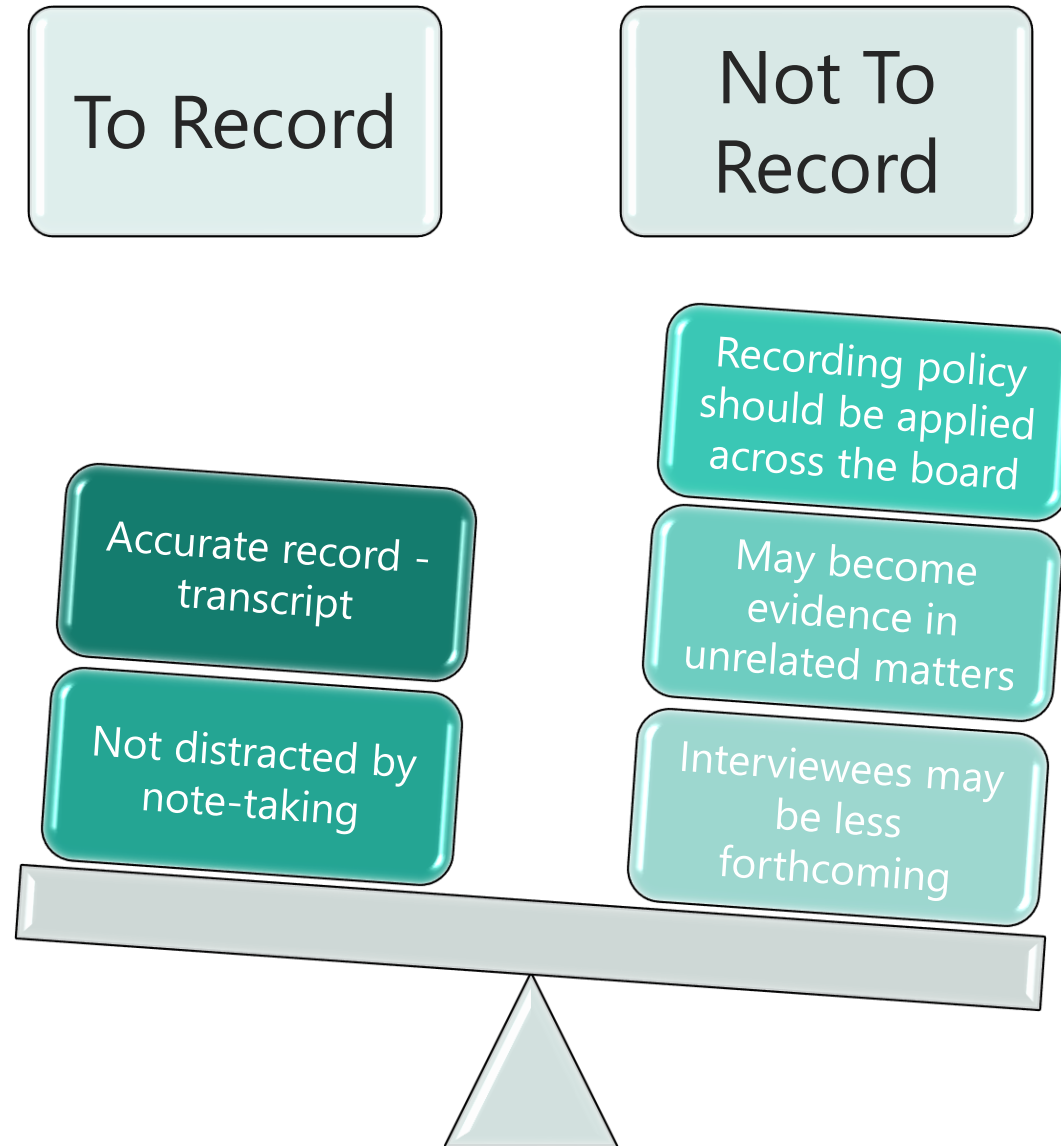
- Are the requests compulsory or voluntary? If **voluntary**, consider:
 - self-incrimination
 - GDPR
 - defamation
 - employment law issues
- Company can face potentially significant legal exposure from the voluntary production of documents, particularly if the provision of those documents is deemed to have adverse consequences for individuals involved.
- If company is **compelled** to provide the documents this will tend to 'cure' above issues.



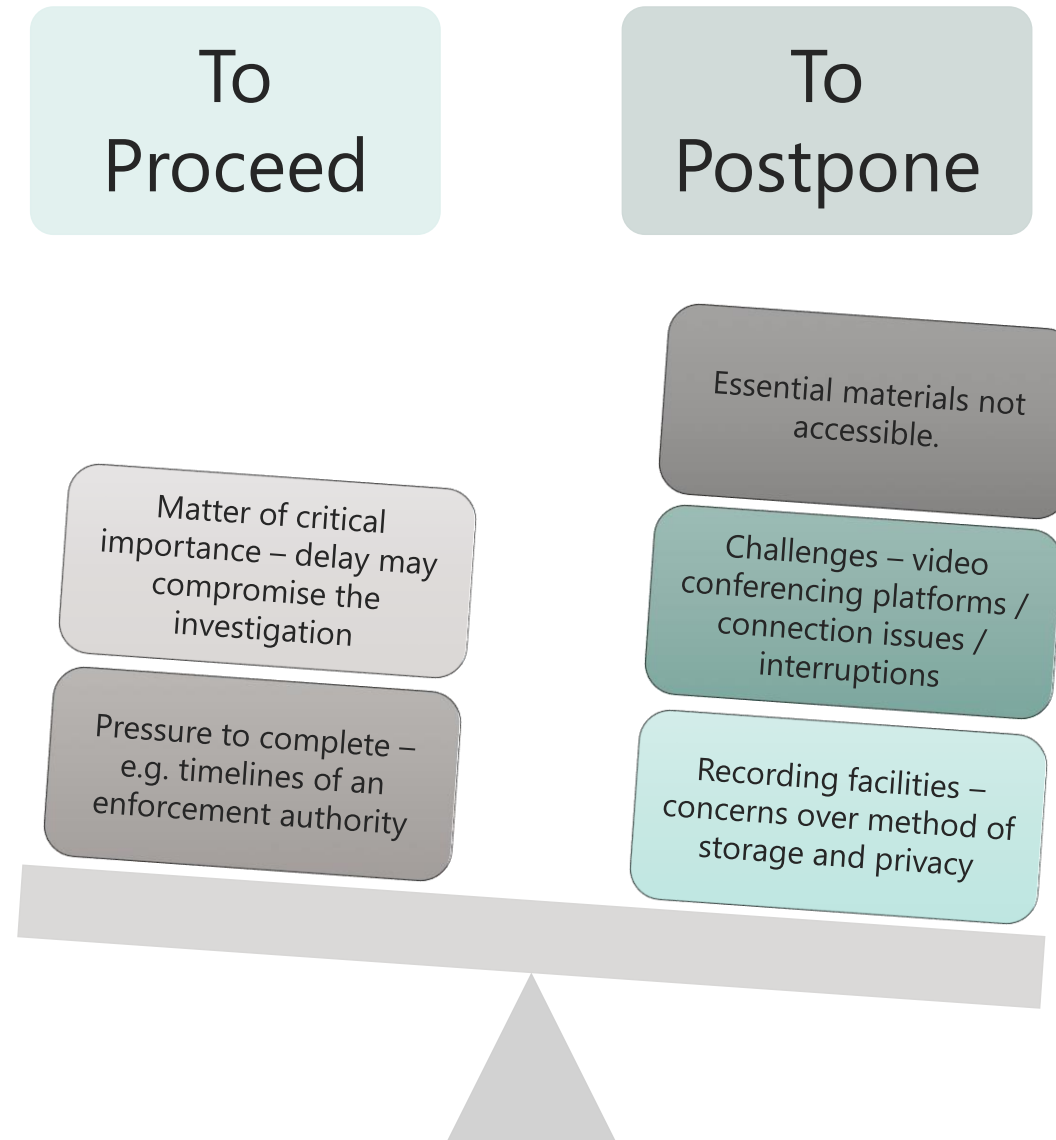
Other Sources of Evidence

- **Covert surveillance** not allowed
- Employer Monitoring – must be **necessary, legitimate and proportionate**
- **Policies (Acceptable Use Policy)**
 - > Emails and internet use
 - > CCTV

Interviews



Remote Investigations during the Pandemic



Completing the Internal Investigation: Possible Next Steps

Produce documents to regulator and respond to its requests

Mandatory reporting obligation / Criminal Complaint

Internal disciplinary procedures

Investigators - Electronic Documentary Analysis

2.2.1 Electronic documentary analysis and disclosure platforms

The document-based nature of much of economic crime means that law enforcement bodies are regularly required to obtain and examine **vast amounts of evidential material**, particularly in the more complex cases. This renders investigations and prosecutions extremely **resource-intensive, causes delays and backlogs, and significantly increases the scope for error**. In this context, a number of agencies represented on the Review Group highlighted the difficulties they face in **not having continuous access to modern electronic document analysis and e-disclosure platforms**. This puts investigators and prosecutors at a disadvantage relative to corporate defendants, who can often afford to engage law firms which use such platforms routinely. All relevant agencies responsible for the prevention, detection, investigation and prosecution of economic crime and corruption should leverage on technological advances to enhance their abilities to carry out their functions.

kmha



Hamilton Report 2020

Key recommendation:

The Review Group considers that all technological solutions that support the detection and investigation of economic crime should be explored including the development of a centralised Government framework for the procurement of state-of-the-art electronic documentary analysis and e-disclosure systems, which could be accessed by the relevant law enforcement bodies (and by the Chief State Solicitor's Office) on a shared basis as required.

Investigators – Documentary Evidence

6.1.3 The volume, complexity and electronic nature of evidential material

This Report has already noted the need for the relevant agencies to be provided with ongoing access to state-of-the-art electronic documentary analysis and e-disclosure systems, in view of the highly voluminous and typically electronic nature of evidential material in a typical corporate crime case. Additional measures that could be taken to support this work could also include:

- Introduce a legal presumption in favour of the admissibility of documentary and electronic evidence to simplify the currently overly complex rules required to prove electronic and documentary evidence.
- Give effect to the Law Reform Commission recommendation¹¹⁷ so that where huge numbers of documents are presented in evidence (especially documents generated electronically), a written summary of such documents may be used.

The Group further notes that the largely electronically-based evidential material in complex economic crime cases, particularly where combined with evolving privacy issues, presents a range of other challenges for investigators, including:

- Encryption challenges;
- Issues relating to the jurisdiction within which the data actually resides;

- The involvement of storage hosts (e.g., Google, Microsoft, Dropbox) and the associated challenges given that these reside in other jurisdictions;
- The limitations of search warrants in the context of production orders, establishing which custodians own which material;
- Issues/risks associated with the use of search terms (by both the investigators and those upon whom production orders have been served).

Privacy issues, and how these interact with the duty to investigate, pose a significant related challenge. In light of recent judgments – and in particular the *CRH* case,¹¹⁸ in which the Supreme Court criticised a particular search by an investigatory body as disproportionate, there is a pressing need for greater clarity on the protection of privacy rights in searches by investigative bodies. There is the need also to establish a process for determining what constitutes irrelevant material in the context of such searches. Technological advances, such as the storage of documents in the cloud, make the case for legislative reform even more compelling.



Hamilton Report 2020

Encryption

- **Law enforcement v. privacy.**
- Encryption is an electronic method used to protect the integrity of devices, data and communications by scrambling the contents preventing its use by persons who don't have the decryption code.
- **Irish position** - Interception of Postal Packets and Telecommunications Messages Act 1993
 - > does not cover the interception of encrypted communications or social media messaging. Garda calls for updated legislation.
- **UK position** – Regulation of Investigatory Powers Act 2000
 - > gives the UK power to authorities to compel the disclosure of encryption keys or decryption of encrypted data
- **EU** – moving towards a ban on end-to-end encryption
 - > the Council of the European Union has reignited concerns from privacy activists that the EU may move towards banning end-to-end encryption or introducing a backdoor.

EncroChat

“DISMANTLING OF AN ENCRYPTED NETWORK SENDS SHOCKWAVES THROUGH ORGANISED CRIME GROUPS ACROSS EUROPE”



“In early 2020, EncroChat was one of the largest providers of encrypted digital communication with a very high share of users presumably engaged in criminal activity. User hotspots were particularly present in source and destination countries for cocaine and cannabis trade, as well as in money laundering centres.”

– <https://www.europol.europa.eu/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe>

“Police say they cracked a secret, global chat system used to plot murders and money laundering and have made hundreds of arrests”

– <https://www.businessinsider.com/uk-police-arrest-746-cracked-encrochat-criminal-service-2020-7?r=US&IR=T>



Thank you



Questions?
