Live Webinar

Demonstrating effective GDPR assurance

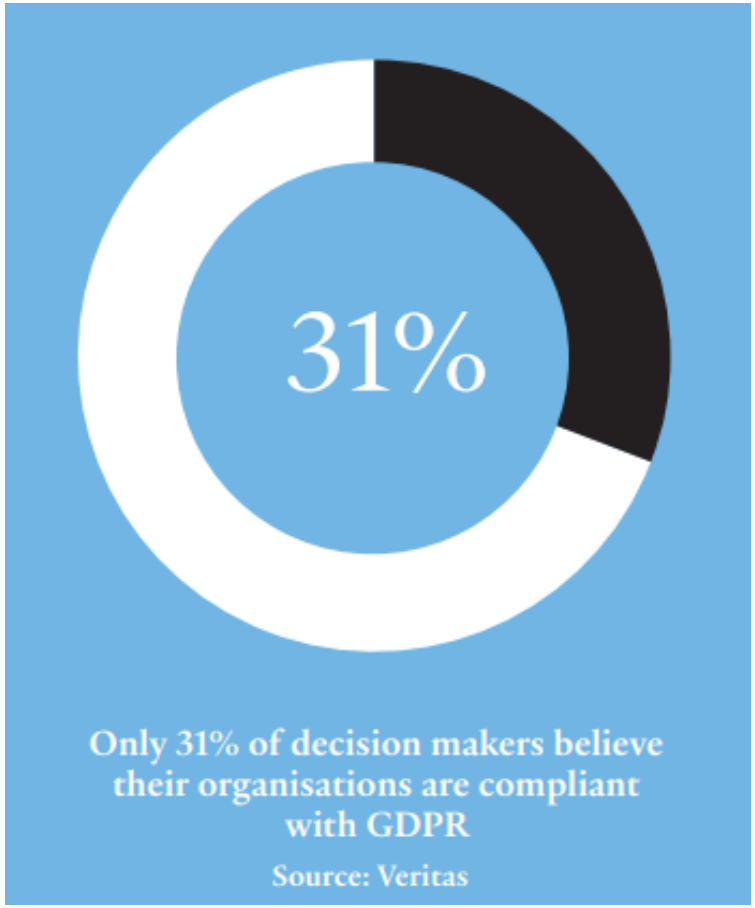
Liz Sandwith - Chief Professional Practice Advisor, Chartered IIA
Tom Faraday - Senior Product Manager, ACL

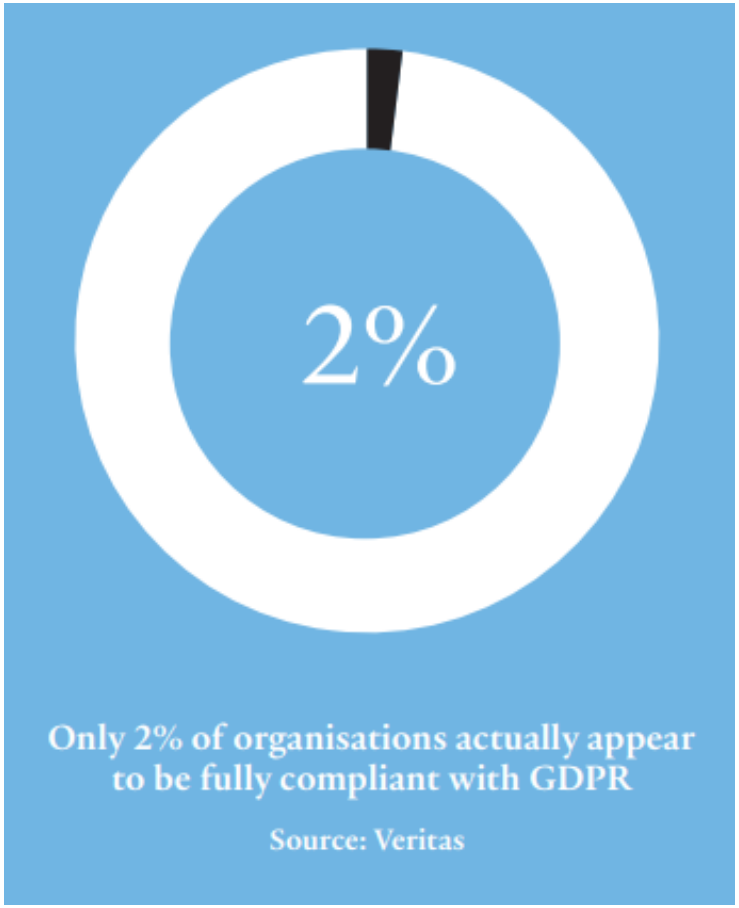
Speakers

Liz Sandwith
Chief Professional Practice Advisor
Chartered IIA

Tom Faraday
Senior Product Manager
ACL

In detail: GDPR and the data protection challenge



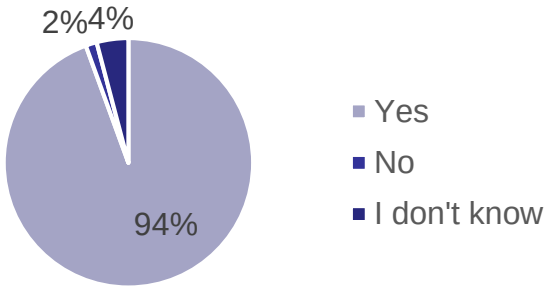


GDPR and the data protection challenge

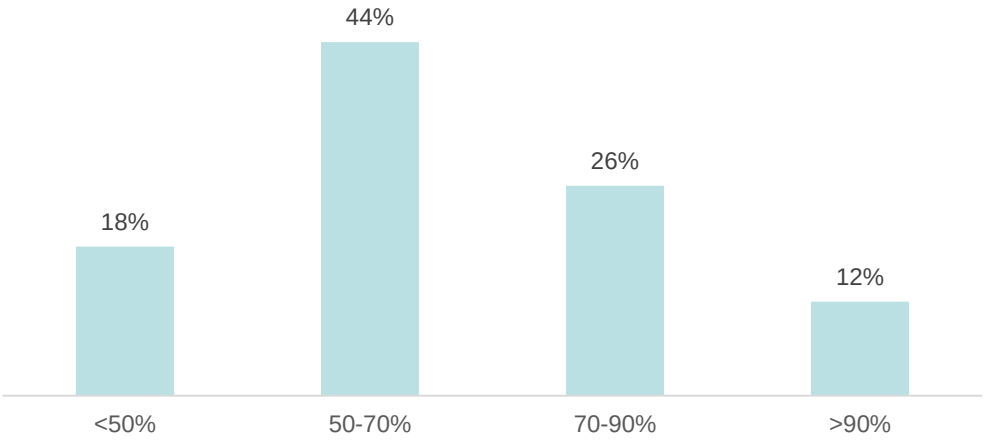
- 31% of decision makers said their organisation was compliant with GDPR, however only 2% appeared to be compliant in an external assessment.
- GDPR is a key concern for three reasons:
  1. Personal data is so pervasive that virtually every organisation holds it, making the scope of GDPR unmatched.
  2. The deadline for compliance on 25 May is fast approaching.
  3. Penalties for failing to comply are potentially huge.
- Boards should have already prioritised GDPR.
- Internal audit is well placed to provide assurance by providing a top down risk assessment of how likely the organisation is to comply.

Live Polling Question #1

- **Is GDPR on your board's radar?**

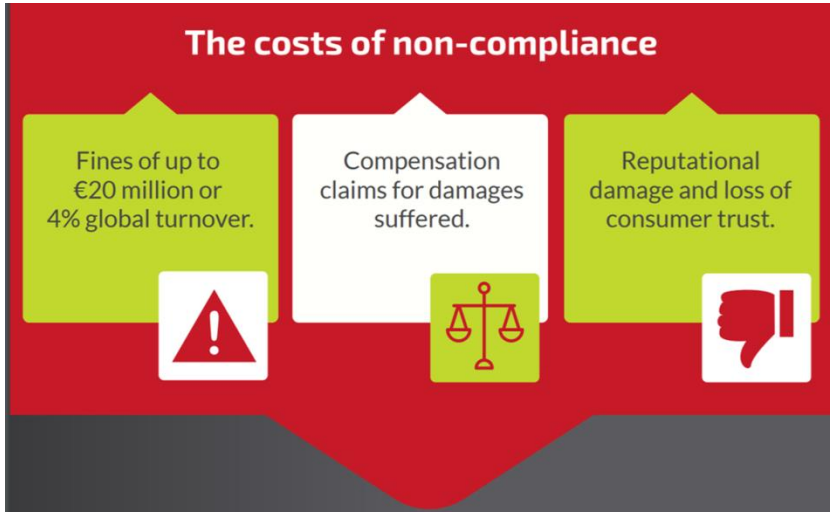


- **As an Internal Audit function, how ready do you feel your GDPR compliance program is?**
  - <50%
  - 50-70%
  - 70-90%
  - >90%



GDPR and the Data Protection Challenge

- Legal and IT teams are already addressing GDPR compliance and internal audit is well placed to provide assurance by conducting a top-down risk assessment of how likely the organisation is to comply, by using gap analysis techniques to review existing controls and identify key areas that require improvement, and by consulting on the practical implementation of new controls and processes.



IT Governance

It is estimated that under GDPR the £400,000 fine issued by the UK's Information Commissioner's Office to broadband group TalkTalk for its publicised data security failings two years ago would have potentially risen to a massive £59m.

7 key internal audit questions

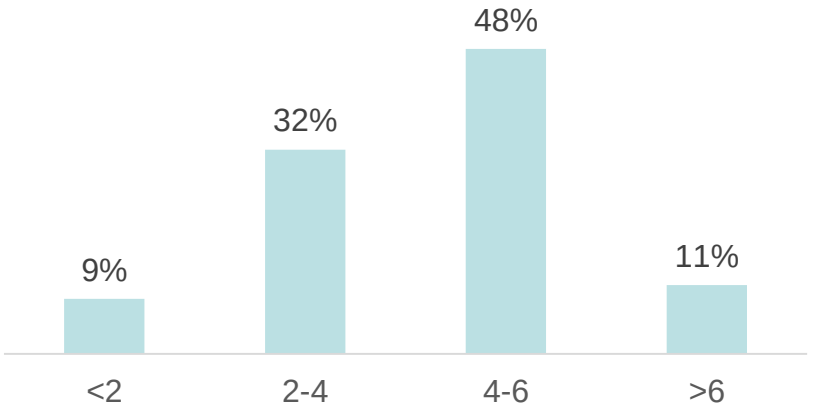
1. What is the readiness status?
2. Where is the information and sensitive personal identifiable information that will fall under GDPR?
3. How will we respond to legal matters e.g. policies and procedures, breach reporting?
4. Is sensitive data protected, stored and backed up securely?
5. How do we identify information for disposition, in accordance with the right to be forgotten?
6. Can we report a breach within the timeline required?
7. How do we reduce our overall risk profile?

Live Polling Question #2

1. What is the readiness status?
2. Where is the information and sensitive personal identifiable information that will fall under GDPR?
3. How will we respond to legal matters e.g. policies and procedures, breach reporting?
4. Is sensitive data protected, stored and backed up securely?
5. How do we identify information for disposition, in accordance with the right to be forgotten?
6. Can we report a breach within the timeline required?
7. How do we reduce our overall risk profile?

How many of these questions do you feel you've already answered?

- <2
- 2-4
- 4-6
- >6




GDPR Roadmap
Step 1
Strategic planning for GDPR in your business
Step 2
Data mapping and audit
Step 3
Policy review and development
Step 4
Staff training and awareness
Step 5
Business support and monitoring for compliance
Step 6
Go live & follow up with on-going monitoring
1
2
3
4
5
6

We are an Enterprise Governance Platform powered by Data Automation

"If management is about running business, governance is about seeing that it is run properly"

- Robert Tricker

Compliance is not a choice and time is short

- GDPR compliance is not just a matter of ticking a few boxes
- The Regulation demands that you be able to demonstrate compliance with its data processing principles.
- This involves taking a risk-based approach to data protection, ensuring appropriate policies and procedures are in place to deal with the transparency, accountability and individuals' rights provisions, as well as building a workplace culture of data privacy and security.
- Rather than panic, you should prioritise tackling those areas where a lack of action would leave your organisation exposed.
- Where an infringement occurs, demonstrating you have made a start could help reduce potential penalties.

How do we know if we are ready?

ICO on-line self-assessment tool, which includes

Step 1	Accountability and Governance
Step 2	Key areas for consideration e.g. consent, children, lawful basis for processing
Step 3	Individuals rights e.g. communicating privacy information, subject access request
Step 4	Breach notification
Step 5	Transfer of data i.e. international

Questions asked in relation to status – not yet implemented or planned, partially implemented or planned, successfully implemented, not applicable

Common Gaps identified

1. Data Protection by default – privacy not yet a priority
2. Rights of data subjects / customers
3. Third party management – data processor
4. Conditions to consent
5. Security of processing
6. Data Breach Reporting and Communication – who needs to be notified
7. Accountability (HR, Compliance, IT and Customer Services, the business, the CEO, Board)

Pragmatic GDPR

Do We Need 100% Compliance?

This new regulation boasts material changes that will intrinsically alter an organization's Data Privacy DNA:

Applies to any org. holding data on EU citizens

Appointment of a DPO

Much higher fines

New rights that empower every Data Subject

Records of Processing Activities

Consent: Clear opt-in for any data collection

Data breaches must be reported within 72 hours

'Data protection by design & by default'

Data protection impact assessments

Accountability

Or a Pragmatic Response to Our Various Audiences?

Management

Regulators

Consumers

Market

Key thoughts – mountain or molehill? Is your business ready to transform?

- **Key privacy risk focus** – highly sensitive data in bulk; consumer data; and processes
- Start **top down** business operations vs. bottom up controls / policies
- GDPR is not an **information security programme**
- **Clarify responsibilities** as a controller and processor
- Privacy may be **disruptive** to digital transformation

The GDPR Solution Landscape

A myriad of different solutions exist to support GDPR Compliance…

Data Discovery
Data Inventory and Mapping
Data Masking

Data Security
Network Monitoring and Security
Application Security

Consent Management
Cookie Management
Compliance Tracking

Survey Tools
Training Management
Case Management
Disaster Response/Continuity

And many more besides…

Companies struggle with...

- Fragmentation
- Lack of Accountability and Oversight
- Difficulties in reporting
- Unnecessary overhead on the business
- An inability to easily demonstrate end to end compliance

As Internal Auditors have we done enough?

1. Have we as internal auditors sufficiently briefed the Board and the Audit Committee about GDPR?

2. **Have we undertaken a top-down risk assessment. What will that do to the delivery of our 2018/19 internal audit plan?**

3. The time spent building relationships with Board and Audit Committee will now be incredibly valuable

4. As internal audit, do we have the ability to support the DPO to drive change and to empower them to act?

5. It doesn't end at May 2018. Moving forward the Board and Audit Committee will require an increased level of assurance around internal control, compliance and reporting processes. Remember, the sword of Damocles is potentially hanging over us all in terms of fines if we get it wrong, make a mistake or take our eye of the ball.

6. Have we done enough? What do we need to do today? **What is the organisation looking for from internal audit in terms of today and going forward?**

Live Polling Question #3

Have you undertaken a top-down risk assessment?

51% Yes

49% Not yet

Is it on your audit plan for the rest of this year to provide assurance over GDPR?

79% Yes

26% No

6 Data Protection Principles – Audit Scope?

In order for internal audit to provide an assurance to the Board / Audit Committee there will be a need for us to undertake a health check audit. The scope for which might include the 6 principles i.e.

Personal data must be processed according to the six data protection principles:

- Processed lawfully, fairly and transparently.
- Collected only for specific legitimate purposes.
- Adequate, relevant and limited to what is necessary.
- Must be accurate and kept up to date.
- Stored only as long as is necessary.
- Ensure appropriate security, integrity and confidentiality.

Don't forget accountability and transparency as an overarching key principles

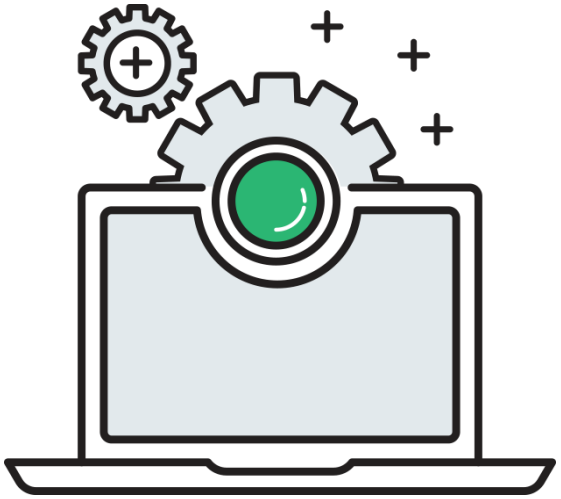
Data-driven GDPR Governance


Focus on...
the data

Simplifying and improving this landscape

The organizational data landscape required to support GDPR is complex, and evolving all the time. Data resides everywhere…

- Systems, databases etc.
- Spreadsheets
- Documents
- Even people



Data is the input and output of each one of the various activities that supports the GDPR program…

Leveraging Data Automation

GDPR Analytics and Automation Considerations

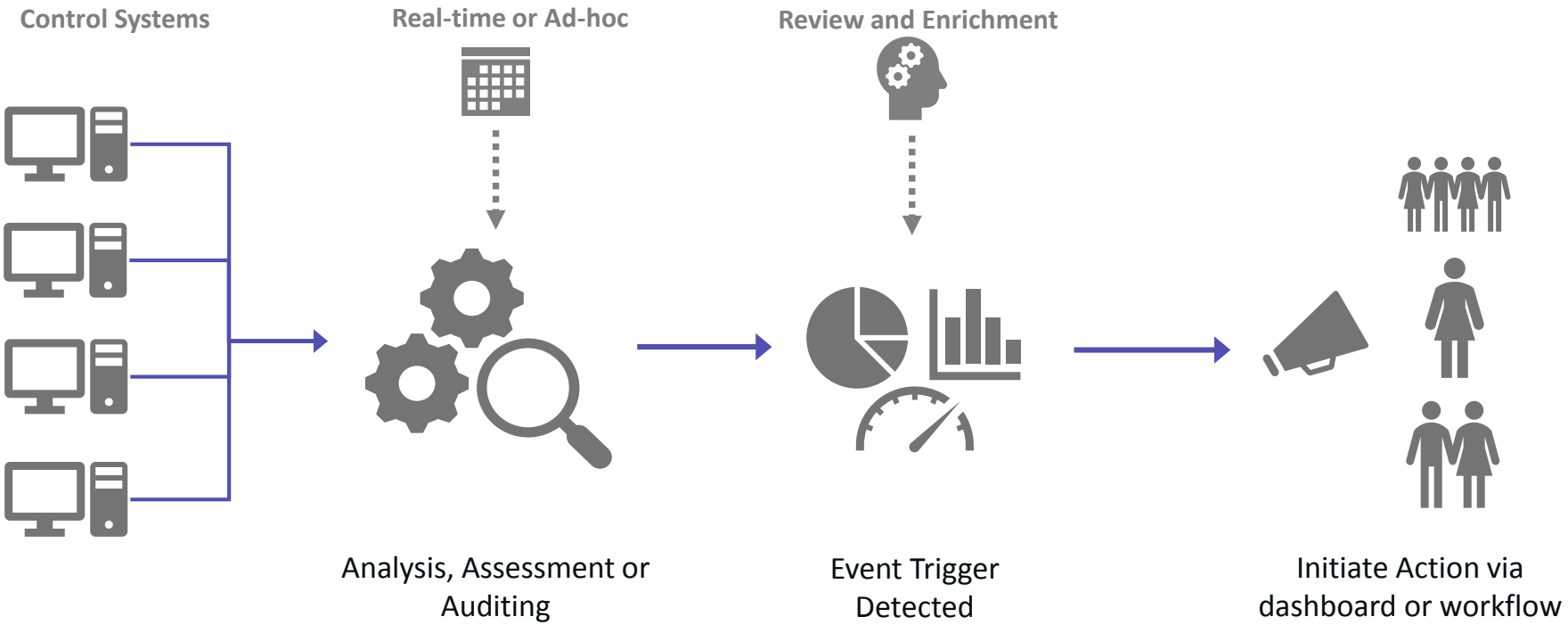
Analysis Inspection Examples

- Inspection for PII keywords or patterns
- Validating pseudonymising approaches
- Risk profiling through control maturity

Active Monitoring Scenarios

- Changes in processor (third party) agreements
- Completion of policy training programmes
- Breach incident monitoring
- Application development lifecycle progression
- Data subject request timelines tracking

Closing the Gap Between Assurance and Action



Data Automation Can Inform and Streamline Compliance

Leverage data automation to:

1) **Inform** the business (and you) of impending compliance obligations and risks
2) Drive adherence to policy with **automated GRC workflows**
3) **Expediate remediation** by alerting the right person for immediate action
4) Automatically manage **prioritization and escalation** paths
5) Compliment manual audit testing with **automated controls monitoring**

Solving the Challenge

- Federate data informing your compliance posture
- Automate tasks activities to drive down ongoing compliance costs
- Surface the appropriate KCIs for monitoring and benchmarking
- Generate perspectives appropriate to the context of the stakeholder
- Track changes and develop awareness of changing obligations

GDPR Compliance Monitoring

Doing an initial assessment is not sufficient. GDPR compliance is an ongoing activity. As a DPO, how will you know when there are items that require your attention?
ACL's platform can provide a single pane of glass view of data from disparate systems and activities undertaken by individual assurance functions. Know and be alerted, rather than guess, when there are issues that you need to deal with.

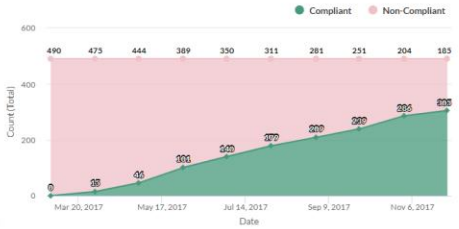
CURRENT GDPR ASSURANCE LEVEL KPI

86%

TIME SINCE DATA BREACH (HOURS) KPI

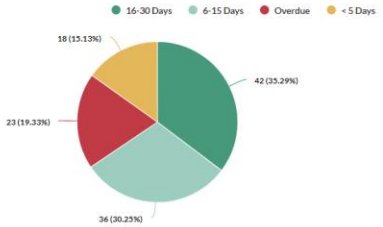
67

GDPR COMPLIANT SYSTEMS

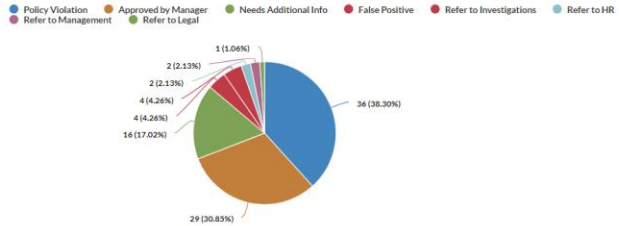


REQUEST VOLUMES BY MONTH

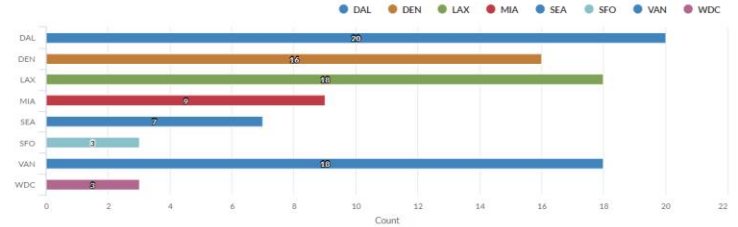
OUTSTANDING REQUESTS AGING



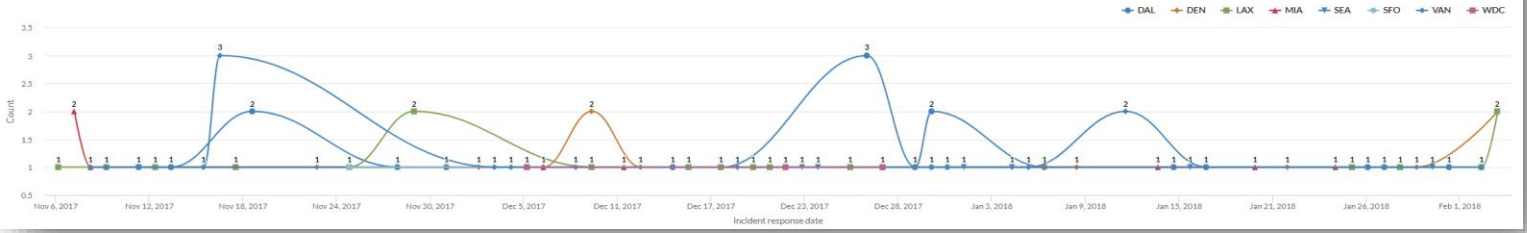
INCIDENT RESPONSES



IT INCIDENTS BY REGION

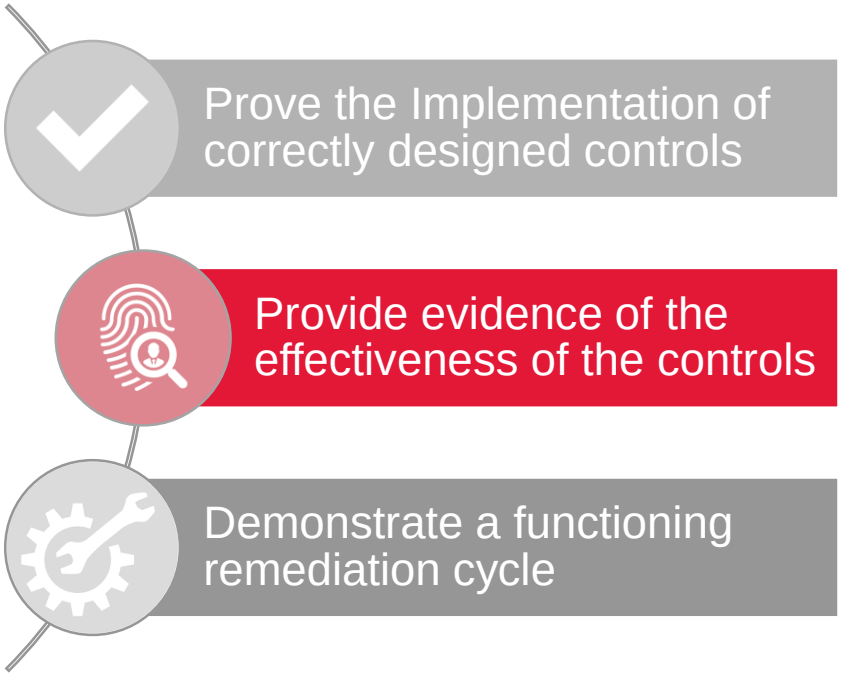


INCIDENT REPORTING TRENDING BY REGION



IN CONCLUSION:

In order to establish a strong defensible position and greater assurance over GDPR Compliance



- ✗ **Existence is not effectiveness**
- ✗ **Sampling is weak**
- ✗ **Subjectivity is risky**

- ✓ **Use Data sources as evidence**
- ✓ **Test continuously and Cover 100% of data sets**
- ✓ **Produce meaningful & comprehensive reporting**

Thank you for your attention!

Questions?

Feel free to reach out to:

tom_faraday@acl.com
liz.sandwith@iia.org.uk