**U8 Lecturecast – Compliance and Security**

Create a security minded culture in company then compliance relatively easy to achieve



**Standards –** ensure systems are compatible and compliant to industry minimum functionality, quality, or security requirements. E.g ISO27002 or ISO9000

**Rules / Regulations –** Other examples of rules / regulations included GDPR IASME NSSC (National cyber security Centre) Standards for Cyber Essentials

**Policy –** Comes from the business. Enforced using business rules, technology and controls – work alongside prescribed or recommended standards.

**Controls –** Enforced through process. Way to apply a framework for ensuring compliance with obligations. E.g COBIT

**Laws –** Works with existing laws and rules. Standards, policies and controls all implemented with regulatory frameworks such as GDPR.

**Compliance**

Compliance helps organisations to consider implications of big data use early in a process. Must consider impact and ensure necessary steps as big data elements move through organisation.

New data types and methods are expected to meet requirements. For example, rapid growth of electronic health records and associated storage, access, sharing and use particularly of personal information.

**Important Compliance Goals**

Ways of keeping big data secure and compliant, technologies available to meet goals of compliance:

1. Control access by process, not job. Stops individuals having too much access.
2. Secure data even when not being used. Sensitive data should be encrypted
3. Protect keys to encrypted data. Save it separately to the data, secure this location.
4. Encrypt more than the data, including applications, services and configurations – protection from malicious users.

**Security Challenges**

Big data must be protected to prevent authorised access, backup or even corruption of data.

Big data can be unique, particularly if accumulated frequently or real time – no way to recreate if lost.

* Access rights control who and what can be access data. More control, better protected but there is a processing overhead for security.

Big data repository has security challenges:

* Access – can be protected if access is eliminated
* Availability – where the data is stored and distributed
* Performance – High levels of encryption, complex security methods and layers can improve security
* Liability – data sensitivity, legal obligations, privacy issues and intellectual property concerns

**Securing Big Data**

* Get rid of data that is no longer needed – should be destroyed as a risk to organisation.
* If it has a value for analytics, must be kept but this could be in an archive, that is only accessed when needed for processing.
* Not all data created equally – some has more value. Traditionally this would be structured data in traditional databases but new big unstructured data stored in different ways may not have the value – challenge to understand and secure this.
* If you can identify the value or need for data can delete or secure it. For example, audit logs may show use of the system but are large and a risk.
* Data can be classified to help with storage plans – personal emails v financial reports for example.
* Backup must consider size and mix of data – transfer speeds and scalability to massive capacities.

**UK GDPR**

Sets out personal data collection responsibilities, sets out the following:

1. Processed lawfully
2. Collected for specific, explicit and legitimate purposes
3. Adequate and relevant
4. Accurate and up to date
5. Kept no longer than necessary
6. Appropriate security

**Article 6 Standards**

Processing of data in a manner than ensures appropriate security. Many standards embedded in organisations to ensure data compliance and security of data.

Standards are developed for compatibility (same set of rules / protocols ae used), quality (minimum level of quality met), trade (Sharing)

Compliance allows trust (process are verifiable), trade (different sectors or areas can trade), regulation (governance of risk and regulation – suitable tools implemented).

**Standards**

**ISO/IEC 27000 series –** ISO (International organisation fort standardisation) IEc (International Electrotechnical Commission) – best practice in info security to prevent attacks on data.

Other standards include ISO 27701 – as a result of GDPR and sets privacy controls

**Activities Requiring Regulation**

**Data Storage –** where data is kept

**Data Processing –** data captured and used as a input then output for further use

**Data Handling –** For all involved in the data and it’s use

**Cross border transaction –** financial and logistic

**Data breaches –** disclosure of confidential, private personal

**Matters and issues relating to disclosure –** disclosure should be lawful

**Authentication and Authorisation of digital identification –** access to data controlled on permission and rights

**Data migration –** transfer from one system to another or where stored

**Privacy matters –** acting in accordance with GDPR

**Most Organisation are affected by regulations** e.g transport, security and legal providers, financial institutions, research organisations, academic and education, business and commercial organisations.