**Unit 8 reading**

CompTIA (2016) *Quick Start to Security Compliance.* - Page 5 / 6

<https://www.comptia.org/content/guides/quick-start-guide-to-security-compliance>

When working on a project should be thinking and discussing compliance from outset. Do not assume others have it covered or there are no requirements.

The Internet of things and other big datasets are non-standard data and not always being considered for security of data or compliance. All data collecting systems must be secured.

Risks and threats to data and systems growing and risk, compliance concerns and security should all be being considered against this background.

Conversations needed to understand business and help understand that technology is a tool not solution to compliance. Understanding business and technology and data being used will help select correct secure requirements.

Cyber Security is made up of many different parts that must come together to build the maturity of the cyber security program.

Article gives the below as examples:

* Documented policies, procedures & standards
* Asset management
* Identity & access controls
* Risk management
* Vendor management
* Physical & environmental security
* Compliance
* Privacy
* Remote access
* Data backups
* Data destruction

ISO frameworks can a help with elements and extent of the above to apply based on business environment and requirements.