Information Commissioner's Office

Cyber Regulation, Resilience and Risk

Heather Toomey
Principal Cyber Specialist

ico.
Information Commissioner's Office

How we regulate

ico.
Information Commissioner's Office

The provision of advice, guidance and tools

Publishing formal opinions and responding to consultations

Undertaking audits and inspections

Issuing recommendations from complaints and breach reports

Mandating changes to practice or processes

Where necessary, issuing reprimands and monetary penalties

Why we regulate

Our aim is to provide regulatory certainty to help organisations comply with legal obligations

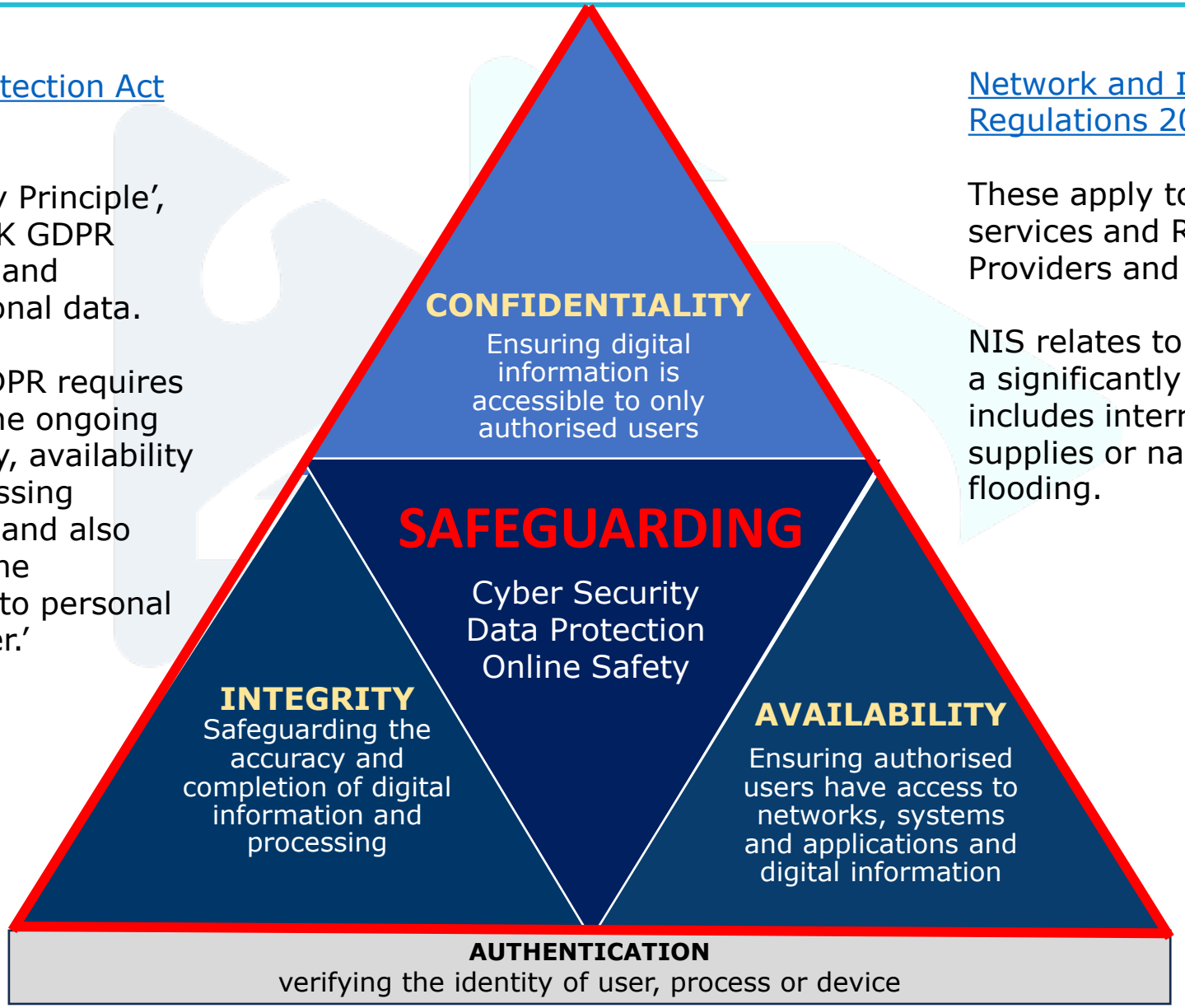
- Safeguard and empower people
- Empower responsible innovation and sustainable economic growth
- Promote openness transparency and accountability
- Develop the ICO's culture, capability and capacity to meet regulatory need

Resilience and the CIA Triad

UK GDPR and Data Protection Act 2018

Known as 'The Security Principle', Article 5(1)(f) of the UK GDPR concerns the 'integrity and confidentiality' of personal data.

Article 32 of the UK GDPR requires 'the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services', and also 'the ability to restore the availability and access to personal data in a timely manner.'



Network and Information Systems Regulations 2018 [NIS regulations]

These apply to Operators of Essential services and Relevant Digital Service Providers and is focused on resilience.

NIS relates to any 'incident' that has a significantly disruptive effect. It includes interruptions to power supplies or natural disasters, such as flooding.

Augustine’s Law 45

One should expect that the expected can be prevented, but the unexpected should have been expected.

Norman Ralph Augustine

Good Governance

- Promote commitment to your organisation's cyber resilience strategy with ALL stakeholders

> "Rank does not intimidate systems. Neither does the lack of rank."

- Have active board-level engagement, adapting your approach if engagement is lacking
- Understand your legal obligations, but also those of third parties you employ
- Undertake regular compliance audits and act on what you find
- Don't rely on certifications but do meet standards, using frameworks where necessary to support this.

Resilience – adapt, overcome and adjust

- Foster a security by default culture and back it up with training
- Understand your risk profile and risk appetite
- Carry out and document risk assessments
- Undertake regular reviews, updating where necessary
- Develop, TEST and iterate incident response and business continuity plans
- Have well documented, well communicated and embedded procedures and protocols
- Agree a communication strategy and alternative ways of working
- Regularly monitor and test systems, looking for evidence of compromise
- Install critical updates promptly, and consider mitigations when this can’t happen
- Collaborate and build your network to leverage expertise you don’t have.

A risk-based approach

The use of emerging, indeed any technology shouldn't be ruled out or feared, but balanced against risk.

- Your organisation may need to implement different measures to those of other organisations, depending on the **level of risk.**
- Avoid benchmarking against other organisations, even if they appear to have a similar structure / operating model / provide similar services. Only you can assess your current state against your target state.
- The best baseline for measuring your compliance, is your own

– **measure** it and **monitor** it.