Security risk management policy

Policy name	Security Risk Management Policy
Date policy was introduced	24 August 2018
This policy has been authorised by (SRO)	Andy Wall, Chief Security Officer
Policy owner	[redacted]
Other contacts	Jason Marsh
Scope of the policy	ONS Security Risk Management
Next review date	24 August 2020

ONS security risk management provides an independent assessment of risk within business operations and Information Communications Technology (ICT) systems and services, taking into account its security requirements. The process identifies security risk in the context of the ONS business activity for consideration within organisational information risk appetite. The process informs a business decision to operate the service or system in a live environment.

All services and systems that handle store and process classified information or business critical data, or that are interconnected to cross-governmental networks or services must be assessed to identify security risk. This ensures that the security risks to the data, system or service are identified in the context of business operations and business Risk Owners are provided with appropriate and proportionate options to mitigate risk to acceptable levels.

The key principle for security risk management is to develop ‘secure by design’ and ‘secure-by-assurance’ services through ongoing involvement in projects from inception, an embedded security involvement in change management and the identification and transfer of residual risk to ONS business areas for ongoing information risk management within the ONS corporate risk framework.

Policy approach

- All ICT services, systems and infrastructure are assessed for security risk through a risk management process in both development and live operations;
- ONS business Risk Owners and the Chief Security Officer (CSO) are collectively responsible for managing security risk within ICT services, systems and infrastructure;
- Security is involved in projects and programmes from an early stage to ensure risk is identified and appropriate mitigations built into solutions;
- Security and ONS business areas review and agree the risk approach and work programme covering their ICT services, systems and infrastructure;
- Security risks and appropriate mitigation options are identified and presented to business Risk Owners for treatment and tracking;

- All ICT services, systems and infrastructure are approved by business Risk Owners to operate in the live environment;
- Security assessments of ICT services, systems and infrastructure are based on the prevailing ONS security approach that incorporates internal, Government, national and international standards and guidance;
- Security assessments of ICT services, systems and infrastructure are performed by trained security professionals working within ONS projects, other project delivery vehicles and live business processes;
- All residual risks arising from assessments of ICT services, systems and infrastructure are transferred to the ONS business area as corporate risks for further management with the support of Security;
- Where significant security risk is highlighted without appropriate mitigation or management activity, this will be escalated to CSO for further action.