Evolving a resilient ONS
2021-2023

Security and Information Strategy

The need for security and information management

The **protection of data is a top priority** for the UKSA. We need to prevent a data breach

So far we have….

Security linked to business objectives

Secure-by-design integrated into digital transformation

Security risk embedded into risk owner decision-making

Nascent estate-wide protective monitoring to detect attack

Office-wide staff security awareness training

Independent validation of approaches

UKSA want to do more

Statistics to support key Government themes, especially from the Pandemic

More and richer data

More sharing and external access

Rapid development of technologies, methods and outputs

Commodity services for platforms

As the threat grows

Security threat is global and evolving quickly

More attacks than ever on Government and the UK

ONS data and systems are a target due to data held

Pandemic fuelled further exploitation through remote working and public fear

Huge range of attackers: staff, criminal groups, hacktivists, hostile nation states

Objectives for resilience

Providing the ability to meet changing business needs while protecting valuable assets

Resilient Behaviours	Resilient Capability	Resilient Operations
Strengthen staff awareness of risk situations and provide the training and tools to enable them to make the right choice in response	Strengthen policy, personnel and services to support transformed business underpinned by continuous assurance to protect services	Strengthen ability for people, processes and systems to adapt to changing business need within an assured operational framework
"Our people do the right thing"	***"We have the right service and support"***	***"The business does not break, it flexes"***
Inclusive Ambitious	**Sustainable** Inclusive	Ambitious **Radical**

The themes

Information visibility

Streamline governance of information and records

Support business to better identify their information assets and status, understand and reduce risks

Tailor elements of information management within Directorates

Business get more efficient processes that provide better MI on their information. Supports improved handling which increases confidence in overall management

Security monitoring

Increase visibility of system and staff actions

Targeted security education with feedback loops from events

Plan for incident response

Speed up technical implementation through devolution

Business get improved safeguarding of data assets and services. Staff will be more security aware and make the right security choice in business scenarios

Risk management

Improved framework to protect staff and services

Right measures targeted at the right assets

Full evidence-based technology assurance

Prepare business areas for resilient operations

Business get more visible security by default, improved policy and guidance, with resilient security services supporting business outcomes

Data management

Quick access to data with some devolution

Full evidence-based data management across all platforms

Improved security training for analysis and research

Data partner assurance statements for trust

Business get more secure and available systems by default, evidence of data management practices and levels of assurance to share with partners, more security aware analytical staff

A new security partnership with the leadership

Different business areas have different priorities that we want to support through **a more extensive secure baseline** that provides **ongoing flexibility** with some **devolution**, but with a safety net creating **resilience**

What do you get?

Ability to adapt your work methods to suit local conditions while meeting secure outcomes

Devolution of some security activity into your business operations

More local decision-making based on improved information about your security risks

Regular information about the security of your operations through management information

Regular review of your security risks and progress to manage them to risk appetite

What's the catch?

Greater responsibility locally to support security and information management outcomes

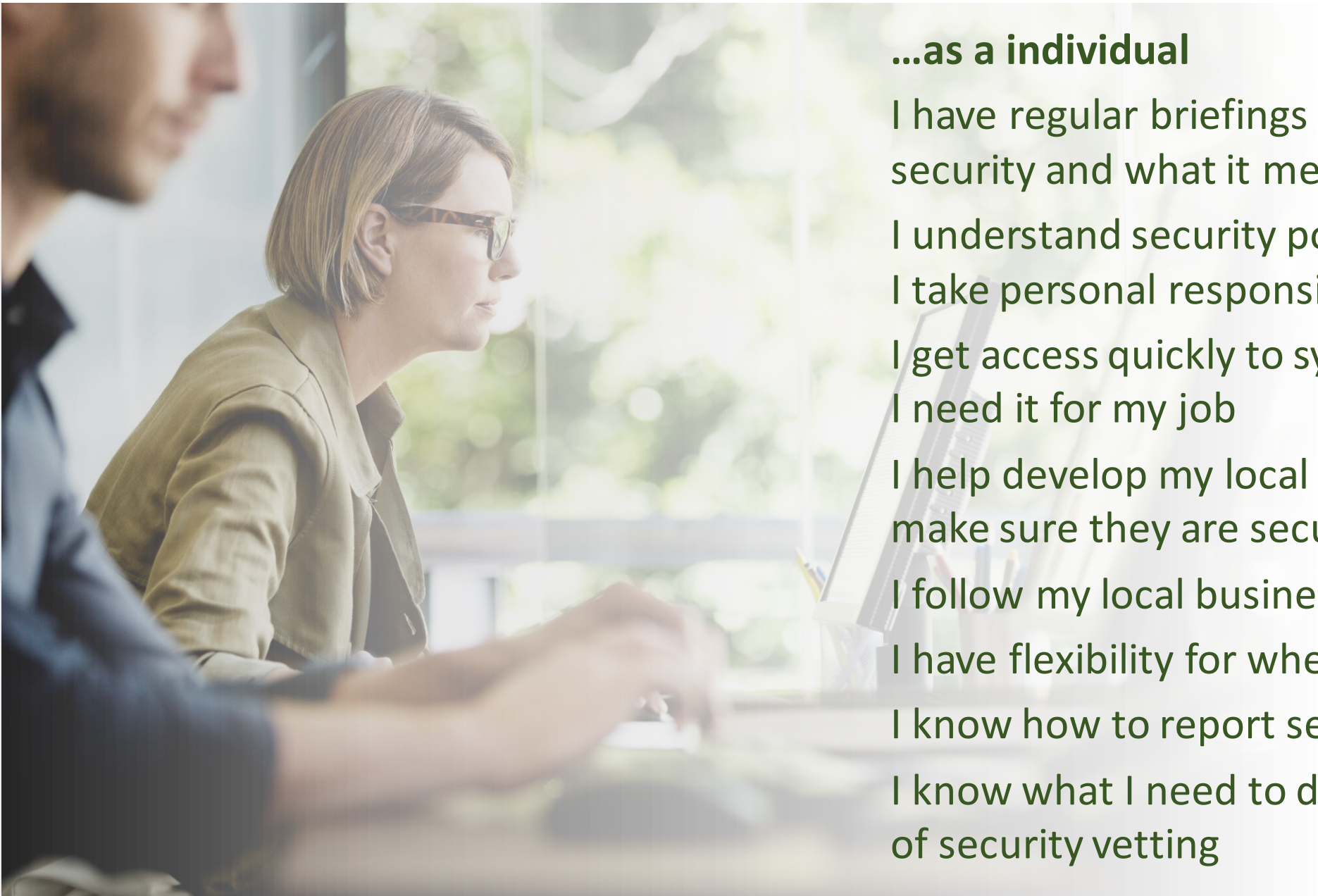
Ownership of the flexibility provided within the security framework

Ownership of security culture within your area to support more secure business activity

Leadership on the security behaviour expectations of your staff

Providing staff the time, training and skills to make it work

What does it look like for me…



…as a individual

I have regular briefings and training about security and what it means for me

I understand security policy and expectations, I take personal responsibility

I get access quickly to systems and data when I need it for my job

I help develop my local business processes to make sure they are secure

I follow my local business processes

I have flexibility for where I work in the UK

I know how to report security incidents

I know what I need to do to maintain my level of security vetting

What does it look like for me…

…as a Manager

I have regular briefings and training about security

I understand the security expectations for my team and I take responsibility for them

I know what information and systems are sensitive

I get information about the security performance of my team, I take action to keep our activity secure

I understand the security risks for my team and the options that I have to manage these

I can change local processes to suit our need and keep them operating within the security framework

I can introduce new projects quickly and get access to these for my team

What does it look like for me…

…as a business leader

I have a dedicated contact point with Security

I have regular briefings and training about security and what it means for us

I get information about the security performance of my business area, I take action to keep our activity secure

I understand how security supports our work and the consequences of an incident

I review our security risks and choose options to keep these manageable

I can change local business approaches to suit our needs and keep them operating within the security framework

I share our security practices with colleagues

When will things change?

Integrated support for security and information advice, design and operations across major ONS programmes

2021

Build updated framework and policies

Create new partnerships with security and the business areas

Set expectations for security in everyday work life

2022

Pilot new approaches for business flexibility

Test more local decision-making based on improved information about risk

Link security to local business objectives

Initial rollout and tweaks

2023

Full rollout and operations across the Office

Thank you for your interest

Read the detail here: