Cloud services will provide business critical functions to government customers and process large volumes of Personal Data relating to staff and citizens.

Any compromise of the Confidentiality, Integrity and Availability of these systems is likely to lead to:

- Distress to individuals
- Reputational damage
- Organisational disruption
- Potential legal ramifications

Cloud services are delivered through a complex combination of organisations and technologies, therefore robust end-to-end assurance is required to ensure security is effectively managed and that supporting controls are effectively implemented.

Security management must be joined up from an end-to-end perspective and managed and maintained to ensure it operates effectively. Having multiple providers will greatly increase the overhead on existing Government internal security resources who may already be over stretched, managing many interfaces without a single provider with overall responsibility.

Having multiple providers greatly increases the risk of security issues arising between demarcation points between organisations.

ISO/IEC 27001:2013 is the latest International Standard for Security Management best practice and organisations that comply or are certified in accordance with the standard have assurance that the security management systems and supporting controls are appropriate and effectively managed.

As a service aggregator Steria has extensive experience of managing end-to-end security for complex services involving delivery through multiple service providers.

The benefits of utilising the Steria ISO/IEC 27001:2013 assessment service includes:

- Increased compliance and support in demonstrating Information Assurance Maturity Model, whilst reducing risks to reputation damage
- Reduced costs and timescales in achieving and maintaining compliance and certification as using tried and tested methodologies and security resource can be drawn on as required rather than having a large in house security team
- Reduce additional strain on internal Government resource through the increased overhead of having to manage security across multiple suppliers
Demonstrable experience of delivering and managing ISO/IEC 27001 Certification alongside HMG accreditation in complex multi-vendor scenarios including Justice, Local Authority, Defence and other central government sectors.

Service Definition

Information security is pivotal in providing assurance to customer stakeholders that their information assets are appropriately protected when utilising Cloud services. Steria has extensive experience of achieving ISO/IEC 27001 compliance and supports delivery of these standards across a number of clients.

Steria has extensive knowledge and capability in this area, and has the following services available on the G-Cloud framework to support consumers with their requirements:

- Information Security Management System (ISMS) Development
- Information Security Management System (ISMS) Operation

ISMS Development

ISMS development requires the production of the key documents that describe and govern the system to enable an organisation to claim compliance and seek certification against the standard.

Steria uses tried and tested methodologies and document templates to support rapid and successful ISO/IEC 27001 Certification and compliance.

Key activities involved in the development of an ISMS include:

- Produce and agree ISMS Scope
- Produce and agree ISMS Policy
- Carry out Risk Assessment and produce risk assessment report
- Carry out initial gap analysis
- Produce Statement of Applicability (SoA)
- Produce security forum terms of reference
- Produce risk acceptance and risk treatment plan
- Produce ISMS procedures

ISMS Operation

In order to maintain ISO/IEC 27001 compliance and certification an organisation must operate and maintain their ISMS to ensure that it is operating effectively and the controls that support it are effective and appropriate.

Steria has extensive experience in providing operational security support to organisations in order to run their ISMS on their behalf.

Key activities involved in the operation of an ISMS include:

- Review operational security reports
- Attend security forums
- Facilitate and attend management reviews
- Carrying out internal compliance audits
- Security incident management and investigation

Summary

Information security is key in providing assurance to customer stakeholders that their information assets are appropriately protected when utilising Cloud services.

Steria take a best practice approach to security management, using ISO/IEC 27001 as the overall management framework, but tailored to support Security Policy Framework (SPF) and Information Assurance Maturity Model compliance.
Steria has extensive experience of achieving ISO/IEC 27001 compliance and certification across Government for complex delivery models involving multiple suppliers and technologies. Specific examples include:

- Maintaining ISO / IEC 27001 Certification and HMG accreditation for the Ministry of Justice - National Probation Service
- Maintaining ISO Compliance and HMG accreditation for the services delivered to the Cleveland Police Authority
- Delivering ISO / IEC 27001 Certification to the Royal Mail Group.

Typical staff roles to deliver this service would include:

<table>
<thead>
<tr>
<th>High Level Job Family</th>
<th>Job Family</th>
<th>Relevant Codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategy and Architecture</td>
<td>Information Management</td>
<td>4-7</td>
</tr>
<tr>
<td>Strategy and Architecture</td>
<td>Information Security</td>
<td>3-6</td>
</tr>
<tr>
<td>Strategy and Architecture</td>
<td>Information Assurance</td>
<td>5-7</td>
</tr>
</tbody>
</table>

A typical ISO 27001 Assessment will fall into one of 3 different sized projects:

**Small (up to):**
- 10 admin staff in scope
- 5 locations
- 4 IT systems
Typically, 30 days effort with an illustrative price of £40,000

**Medium (up to):**
- 40 admin staff in scope
- 10 key locations
- 10 separate IT systems
Typically, 55 days effort with an illustrative price for this type of service is £73,000

**Large (up to):**
- 100 admin staff in scope
- 25 key locations
- 40 IT systems
Typically, 80 days effort with an illustrative price of £105,000

This and other Specialist Cloud Services will be charged in accordance with our rate card for Lot 4 Specialist Services, please see the Steria SFIA Rate Card.

If you require a different commercial arrangement such as fixed price or output based charging, please contact us to discuss your requirements at g-cloud@steria.co.uk
About Steria

Steria delivers IT enabled business services and is the Trusted Transformation Partner for private and public sector organisations across the globe. By combining in depth understanding of our clients' businesses with expertise in IT and business process outsourcing, we take on our clients' challenges and develop innovative solutions to address them efficiently and profitably. Through our highly collaborative consulting style, we work with our clients to transform their business, enabling them to focus on what they do best.

Our 20,000 people, working across 16 countries, support the systems, services and processes that make today's world turn, touching the lives of millions around the globe each day. Founded in 1969, Steria has offices in Europe, India, North Africa and SE Asia and a 2013 revenue of €1.75 billion. Over 20%(*) of Steria's capital is owned by its employees. Headquartered in Paris, Steria is listed on the Euronext Paris market.

(*): including “SET Trust” and “XEBT Trust” (3.90% of capital)