Securys®

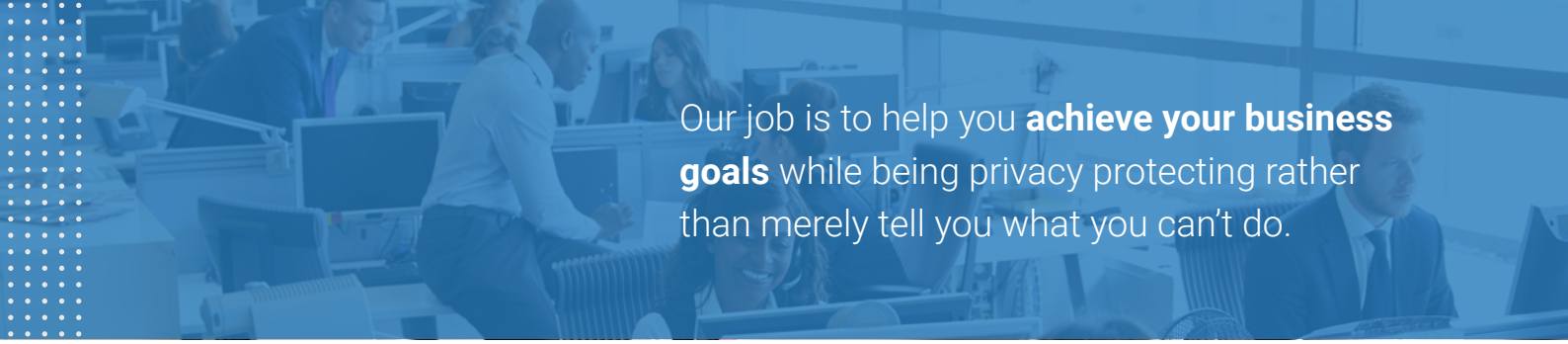
Data privacy audit process

A data privacy audit is the foundation on which a company organises its data protection compliance.

Here at Securys, the specialist data privacy consultancy, we are more practical and more hands-on than other consultants; we are not merely advisors but also implementors. Our job is to help you achieve your business goals while being privacy protecting rather than merely tell you what you can't do.

We are business analysts as well as privacy consultants. We won't give you dry, theoretical advice that can't be implemented; we make sure that what we recommend can actually be delivered on the ground with a positive impact on your business, and we'll deliver it.

Privacy Made Practical®

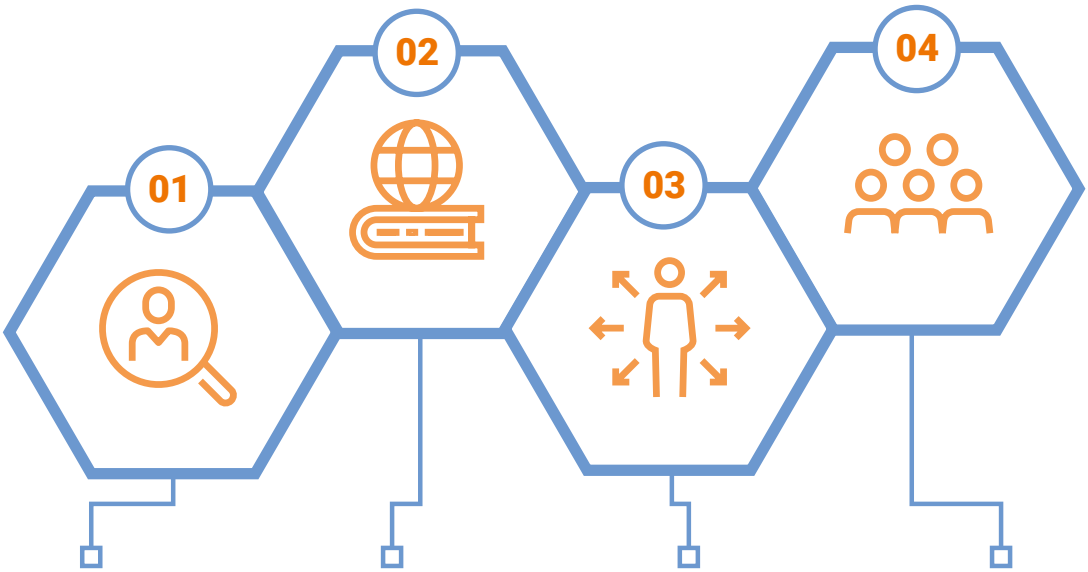


Our job is to help you **achieve your business goals** while being privacy protecting rather than merely tell you what you can't do.

Our four-step plan to becoming your privacy engine room

Our proprietary tools and methodologies help us do all of this dynamically, quickly, and efficiently. We know that privacy audit clients don't want to wait months to be told their key risks and opportunities, so we've developed Surface Risk Scoring™ which enables us to rapidly identify priority areas. This means we can begin addressing critical risks while continuing to complete the audit.

The compliance journey



AUDIT AND DISCOVERY

Gap analysis

Discovery interviews

Surface risk scoring

REPORT

Data catalogue and RoPA

Risk dashboards

Remediation recommendations

REMEDIATION

Detailed assessments

DPIA, LIA, TIA

Implementation support

Breach management

PRIVACY OFFICE

Privacy by design

Privacy operations

Advice and training

OPTIONS

Training

Point Projects

DSAs
Vendors
BU-specific remediation
DSAR support

Privacy Made Positive™

Discovery and risk scoring

The audit and discovery phase combines policy and document gap analysis with interviews and business analysis to give you an accurate picture of risk. The report sets out detailed remediation recommendations which we implement in collaboration with you in the remediation phase. This includes, but is not limited to, regulatory paperwork, supplier assessments, contract reviews, training, policy drafting and privacy notices.

The audit process

Gap analysis

Gap analysis comparing existing documentation, policies and procedures to regulatory requirements and best practice.

Questionnaires and interviews

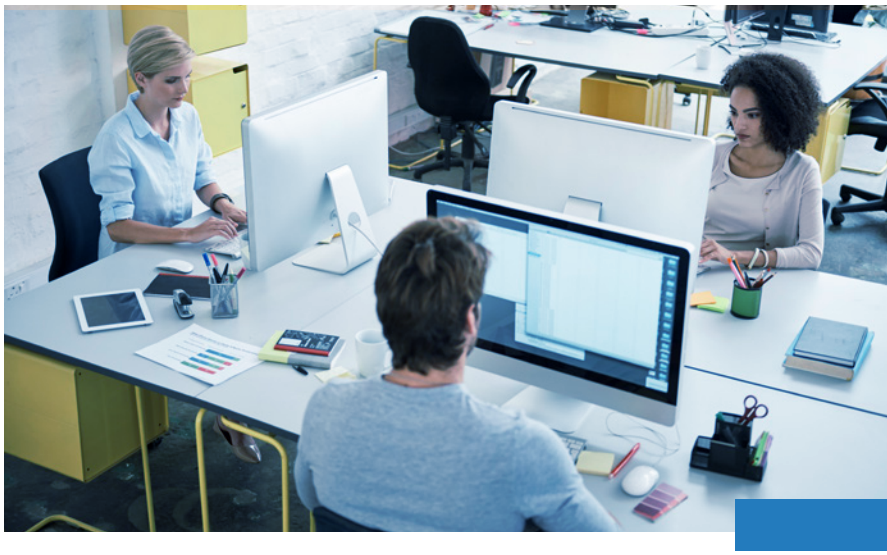
Questionnaires to key staff from the boardroom to the shop floor, followed by interviews to understand how data are used.

Follow-up emails

Follow-up emails and calls for clarification and to allow your staff to share insights arising from their new understanding of privacy.

Gap analysis

Effective compliance and good data protection practice starts from comprehensive and well-understood documentation. We review your existing privacy and information security policies, procedures, notices, logs, and assessments and compare them to best practice and regulatory requirements. This helps us to better understand your business, assess where improvement is needed and understand your existing privacy and information security provisions so that we can limit the questions asked in the next phase.



Questionnaires and interviews

We follow up with questionnaires to identified key individuals, from the most senior executives down to the people who deal with data day-to-day. The questionnaires are followed by interviews – for those who have significant responsibility for data, or who need support with the questions. These interviews are informal: we call them “data protection therapy” and are a two-way street; they don’t just help us build our understanding of your data processing practices but also act as privacy awareness sessions and open Q&As for your staff.

This phase has three objectives:

- Assess the level of privacy awareness
- Fill in gaps from the existing documentation
- Determine whether policies and procedures are being followed in practice

Vendor assessment

As part of the discovery process, we will look at your existing vendor compliance management, sampling vendor contracts to check for appropriate data protection provisions and assessing supply chain risks to data and information security.

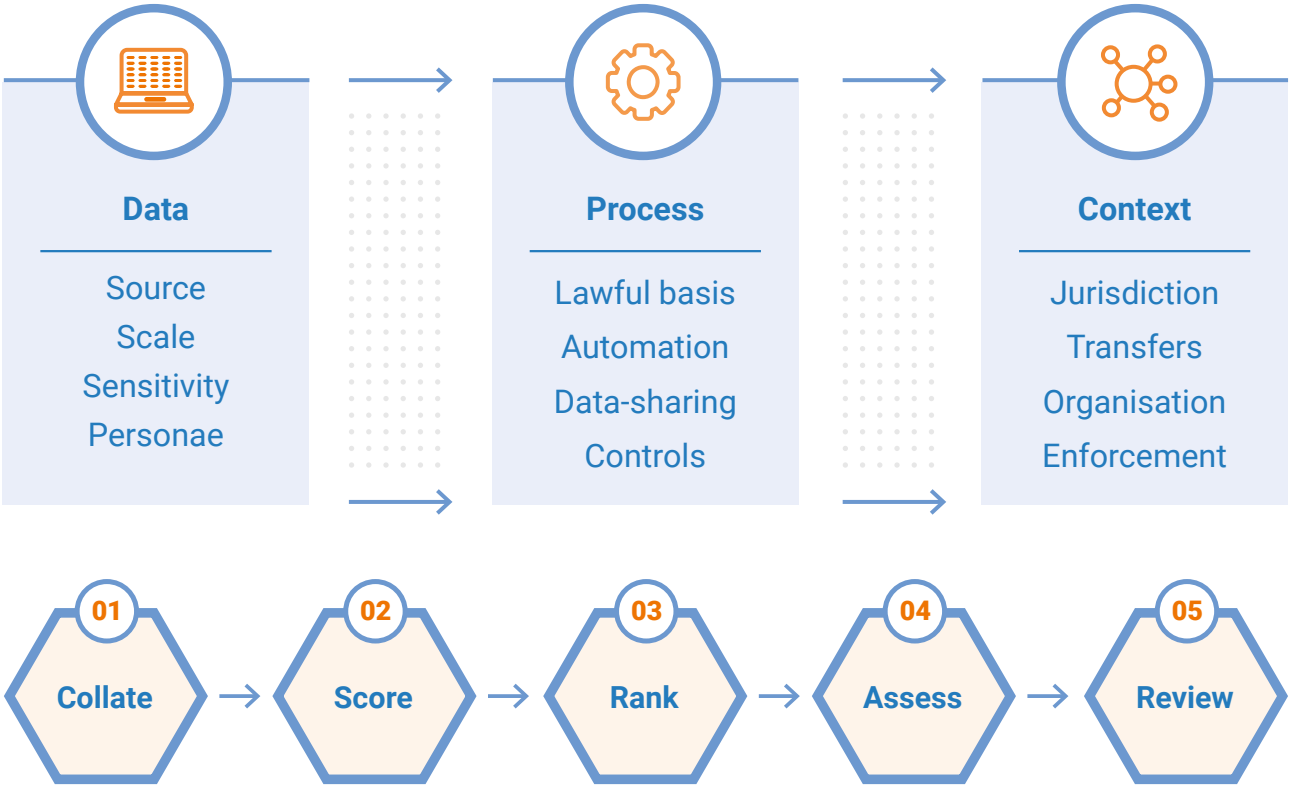
Surface Risk Scoring™

As we work through the discovery and audit process, we are continually updating your Surface Risk Scores™ based on the results and our emerging picture of your organisation and its data processing. This produces an evolving dashboard highlighting your key risks and opportunities with practical recommendations for action.

The process

- Rapid process based on existing documentation, observation and review
- Gather 15-20 data points across all personal data processing purposes
- Score for risk and rank
- Target top 10%
- Assess and review

Securys Surface Risk Score™ – looking for risk and opportunities



Surface Risk Scoring™ combines a number of carefully chosen data points about each process, considering impact and likelihood. We assess impact though two lenses:

- The lens of impact on the data subject, whether through successful processing or failure including confidentiality breaches, inaccuracy, or loss of availability.
- The lens of impact on the organisation – including reputation risk, potential for litigation, commercial effects on customer and employee loyalty and engagement and of course the possibility of regulatory action.

When considering likelihood, we're also thinking in more than one dimension. A variety of real-world factors can increase likelihood, including the political climate, regulatory focus and shifts in prevailing criminal activity. By the same token, we're looking for factors that can reduce the probability of a risk being actualised, whether that's effective controls, positive awareness and engagement or minimisation of data.

We create a visual plot of the results ranked against likelihood and impact; processes in the top right areas of the grid represent your priorities for remediation and improvement.

The Securys plot of impact vs likelihood of privacy risk

Benefits of risk plot analysis

- Looks at factors affecting impact and likelihood of privacy risk
- Allows subsequent phases to focus more detailed assessment of high risk processes

Compliance with privacy regulation is a journey, not a destination. No organisation is ever perfectly compliant, and you will always have some processes that are less compliant than others. So, we always recommend using a risk-based approach to prioritise remediation efforts.

We think of it as eating an elephant, you have to start somewhere and take small mouthfuls. The object of Surface Risk Scoring™ is to help you work out which bite to take first.

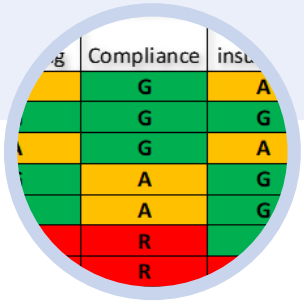
Reports and outputs

Alongside the Surace Risk Score™ grid we provide:

01

A Red, Amber, Green dashboard

A visual RAG dashboard showing you the distribution of privacy risk by business function and aspect of privacy; this helps you spot risk concentrations and areas of concern, but also highlights good practice and centres of excellence. This dashboard is updated continuously through the remediation phase to provide you with clear and easily reported evidence of positive impact.



02

A data catalogue and Record of Processing Activity

These form the fundamental basis of your privacy practice, act as part of your required regulatory paperwork and allow you to develop appropriate functions for dealing with data subject requests. We can provide these documents in our own templates or in OneTrust® depending on your organisational requirements and capabilities.

03

Remediation recommendations

A detailed set of remediation recommendations, grounded in practical applicability and supported by our commitment to work with you to implement them. Risk-prioritised and clearly differentiated between regulatory requirements and best practice improvements, the report is written in business language, built on our knowledge of your business, and aimed at your audience.

For more information and a no-obligation initial consultation, please contact Securys at info@securys.co.uk.

Why Securys?

We're not just a consultancy. **We're your privacy engine room.** We can stand in your boardroom and do strategy with the best of them, and work with your compliance teams to solve knotty problems. We can audit your compliance and deliver drillable risk dashboards across the organisation. But above all, we can get involved at ground level and help your frontline teams get the job done. That's Privacy Made Practical®.

Securys®
Privacy Made Practical®

T 0800 193 8700
E info@securys.co.uk
W www.securys.co.uk

securys-limited

UK0011/0122

Our services

Securys provides a range of specialist services. To find out more and to arrange a free initial conversation please get in touch by emailing info@securys.co.uk.

Compliance management

- DPIA - Data Protection Impact Assessments
- Privacy notices – public, employee, counterparty
- Cookie banners and website compliance
- Consent wording, consent logs and management
- Breach logs
- LIA - Legitimate Interest Assessments
- TIA - Transfer Impact Assessments
- RoPA - Record of Processing Activity
- Data catalogue

Privacy Office as a Service

- Privacy advice and support to functions and BUs
- Breach management
- Data subject complaints and communications
- Regulator communication and negotiation
- DSAR - Data subject access requests
- New project support including privacy and security by design and by default
- Vendor selection, due diligence, and management
- Data sharing agreements and standard contractual clauses
- Data retention policy design and enforcement
- Data classification and sensitivity design, labelling and enforcement
- Development and maintenance of internal privacy and processing guidelines
- Advice and support on management of sensitive data, including health programmes

Privacy consultancy

- Privacy audit, including BCR verification
- Privacy gap analysis and benchmarking
- Privacy risk assessment and remediation recommendation
- Internal and external data flow mapping
- Design and implementation of Privacy Operating Model
- Privacy remediation: support and execution
- Business Analysis and Business Process Reengineering
- Project Management for privacy delivery
- Advisory: advice on legal interpretation, lawfulness, international regulation
- Litigation support
- Governance: design and implementation of internal audit, reporting and KPIs

Data Protection Officer as a Service

- Appointed DPO or EU representative as required
- Data subject and regulator liaison
- Advice on and governance of data processing
- Compliance review and audit
- Information security consultancy
- Information security audit
- Information security gap analysis and benchmarking
- Information security risk assessment and remediation recommendation
- Technical standards review
- Data loss prevention

Information security governance programme design and implementation

- Incident management and incident support
- Technology selection and implementation oversight
- Supplier management

Certification

- ISO 27001 & 27701 certification gap analysis, preparation and support
- PCI-DSS gap analysis, preparation, support and maintenance

Training (in-person, remote, recorded)

- C-level workshops on privacy implications, governance, infosec
- User privacy and security awareness training
- Privacy professional training for CIPP/E/A & US, CIPM, CIPT
- International privacy regulations
- Train the trainer

Licensed material

- Complete Privacy and Information Security Management System (ISO27x01)
- Individual policies and procedures for privacy and information security
- Training videos, handouts and supporting material

Platform support

- OneTrust® implementation and operational support
- Privacy and security compliance in Office365®