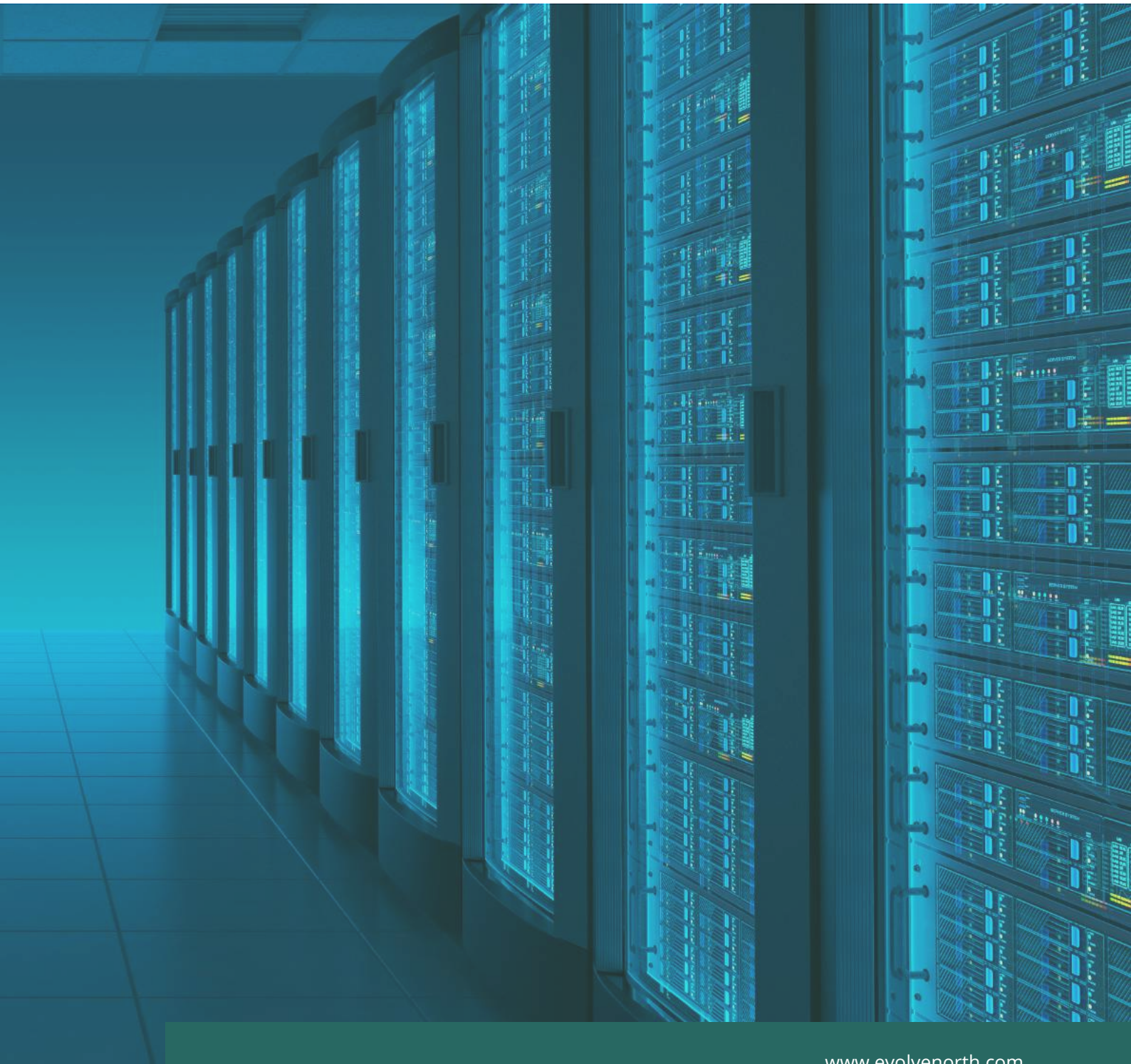
evolvenorth

Services Guide

Governance · Compliance · Assurance

www.evolvenorth.com

[1]2018 Hiscox Cyber Readiness Report



About Us

Our office is nestled in the small market town of Richmond, North Yorkshire, gateway to the Yorkshire Dales.

Evolve North was formed in 2004, our highly experienced team has an exceptional track record of delivering sophisticated solutions into complex environments

We have skillsets covering both IT Security and Information Governance disciplines, which allows us to address the whole of your business and ensure that no gaps exist in your Information Security Management System. Since we can facilitate such a wide spectrum of services, you and your business can enjoy the peace of mind that your systems are fully safeguarded.

Our clients describe us as professional, knowledgeable and above all straightforward in our approach. Even some of our largest clients work in small and sometimes under-resourced teams and we recognise your time is extremely precious. Evolve North is often regarded as an additional member of our clients' teams, helping busy DPOs and IT Managers communicate their policies and choices in a simpler way. This straightforward approach helps clients understand their risks and communicate strategy, benefits and outcomes effectively to their senior management teams.

Our exceptional Information Governance experience is allied with our IT Security skills which include firewalls, encryption, multi-factor authentication, anti-ransomware, anti-malware, identity and access management, penetration testing, vulnerability scanning, web and email filtering and security incident and event management. We provide the complete Information Security Management System approach.

Company Contacts

We welcome you to contact us with any enquiries you may have regarding our services or your data protection needs

Below you can find contact details for general enquiries as well as direct contact details for company directors, you are invited to contact us with any enquiries you have regarding the services in this booklet or the many other data protection services we have to offer.

General Enquiries

EMAIL

info@evolvenorth.com

PHONE

01748 905 002

ADDRESS

Evolve North
40 Newbiggin
Richmond
North Yorkshire
DL10 4DT

Company Directors

MARK DENNIS

Managing Director

07968 537 115
mark.dennis@evolvenorth.com

DAVID MOFFATT

Technical Director

07515 754 491
david.moffatt@evolvenorth.com

PAMELA THOMPSON

Financial Director

07751 150 734
pamela.thompson@evolvenorth.com

Our Industries

Evolve North work across a wide range of differing industries throughout the UK and Europe in both the public and private sectors

FINANCIAL SERVICES

We have worked with a very diverse range of financial institutions from independent financial advisors through to building societies and financial software developers to help deliver a range of technical, information governance and compliance projects.

HOSPITALITY

No matter the size of the organisation, we understand how important it is to maintain a secure environment for storing your guests' personal information. We have delivered myriad data security projects for a variety of hotel clients from large chains to bespoke luxury hotels.

EDUCATION

Primarily in colleges and universities, we have developed, managed and delivered a range of IT security and information governance projects. Providing reliable, secure and appropriate services to students and staff is vital to the performance of an educational institution.

TRANSPORTATION

Planes, trains, ships and logistics, we have delivered services across very diverse transportation environments. We understand the constraints, challenges and often unique security requirements within the transportation environment and can use our experience to support you.

HEALTHCARE

We are one of only a handful of external consultancies to deliver information governance services into the NHS, including guidance on the Data Security and Protection Toolkit, data protection impact assessments. Our expertise and knowledge in the NHS is second to none.

LEGAL AND LAW

Ranging from independent solicitors through to large corporate specialists, we have worked closely with a number of legal and law practices and are experienced in dealing with the close levels of scrutiny organisations in this field are subject to.

NOT FOR PROFIT

We have worked with charities, housing associations and other not for profit organisations and understand how important confidentiality is within these realms. We seek to help protect you and your clients from private information becoming public.

LOCAL GOVERNMENT

Our streamlined approach to project delivery and development has enabled us to work closely with Local Government organisations across the UK delivering information governance and technical solutions that comply with exacting regulatory and financial requirements.

Our Services

Our extensive experience in the field of data protection has allowed us to develop the services businesses need to stay secure

You can read about some of the many governance and security services offered by Evolve North on the following pages. Customers with any other data protection needs, including policy and procedure development, training, data mapping and IT security, are encouraged to contact us to find out how we can help.

Breach Management

We can provide Information Governance and IT Security consultants with many years of experience to manage your breach or loss incidents

We've all read about them in the media, but what do you do if you experience a data breach? It is not a time to panic. Don't rush into taking the wrong steps, digging a bigger hole for your business to get out of. Making a rash decision may make the situation worse. We can help you limit the damage to your organisation, your customers, and your reputation.

Data breaches can come in all shapes and sizes, whether it is a small breach involving the loss or disclosure of one person's information, through to a wide-scale cyber security attack on your key systems. Evolve North skills in IT Security and Information Governance can help you contain, manage and learn from these incidents.

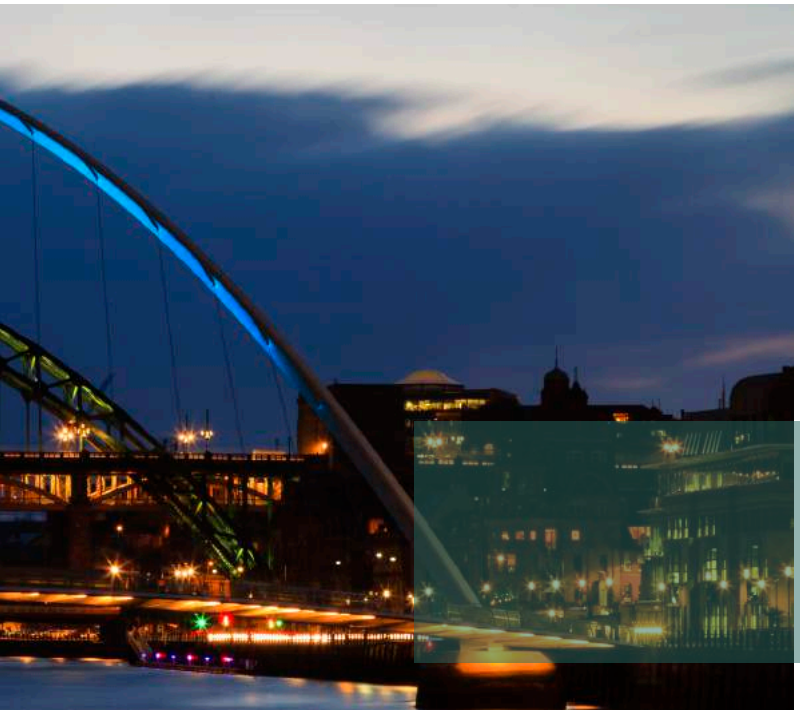
Ensuring prompt containment and remediation is key to managing breach or loss. Ongoing communication with the Information Commissioner and Data Subjects helps to ensure you remain compliant with the Data Protection Act and GDPR.

Evolve North can provide breach and incident management, on either an ad-hoc basis or as a monthly subscription

assurance service, keeping you safe in the knowledge that at your time of crisis, there is a team of professionals on-hand to support you.

Our consultants have managed multiple breach and loss incidents, including working with the Information Commissioner's Office and PCI DSS, all have many years of experience in Senior IT Security and Information Governance roles, working within the NHS, Financial Services, Hospitality and Transportation.

But it's not just about reacting to a breach, Evolve North can help you effectively minimise the chance of incidents and implement effective breach management approaches when they do occur. We can help you develop effective information risk management programmes to help identify where risks may occur, how to mitigate these risks and effective controls to put in place. This will give you the assurance that you are doing all you can to prevent data breaches occurring in the first place. And should the worst happen, we can support you in developing effective Data Breach Procedures and Cyber Incident Response Plans so that breaches are handled appropriately and in line with current legislation.



72-Hour Countdown

All organisations are required to report breach or loss of personal data within 72 hours under the Data Protection Act and the GDPR.

Failure to do so can result in a significant monetary penalty and further prosecution of the Officers of the business.

Our breach management service at a glance...

- **Breach Reporting**
  We'll advise you whether your breach needs to be reported to the ICO and give guidance when reporting and responding to the ICO and Data Subjects.

- **Remediation**
  Remedial advice is provided for the breach or loss, including hands-on support when needed.

- **Informing the Data Subjects**
  We'll support you with the creation and management of effective communication, helping you to inform affected data subjects of the potential impact on them while minimising the potential reputational damage your business may incur.

- **Breach Policies**
  We can help you create effective Breach Policies and Procedures to ensure all staff know how to respond to data breaches.

evolve north

Data Protection Compliance Reporting

We'll review your current adherence to data protection law, ensuring you have a clear and concise view of your current compliance status

A review of your current compliance with data protection laws will allow your organisation to identify any existing risk areas that may need further action and demonstrate that you are actively meeting your legal requirements in relation to personal data. We can produce a remediation plan that can be used for ongoing improvement planning within your organisation.

We have experience in producing gap analysis reports, identifying the current status of organisations across many industries and geographic locations, and we understand the work required to become compliant with the relevant laws, regulations and standards governing organisations around the world.

Our gap analyses routinely take into account the many and varied requirements of the following: UK Data Protection Act, the EU GDPR, the NIS directive, the Human Rights Act, PECR, PCI DSS, ISO 27001 and ISO 9001.

Our data protection compliance reporting service at a glance...

Documentation and Analysis

We'll perform gap analyses, risk assessments and staff interviews to identify the gaps in your organisation's compliance.

Feedback to Key Accountability Structures

We can present our findings to the Board, Senior Management Team or any other relevant group.

Ongoing Remedial Support

We're here to help you absorb the contents of your compliance report and support you in implementing appropriate actions where gaps in compliance have been identified.

Our Approach

Our approach to Data Protection compliance reporting will be tailored to the needs of your organisation. We will work with you to understand what these requirements are and provide a bespoke solution based upon them.

We help global organisations align their business policies with local regulations around the world

We can support your organisation in ensuring its local compliance as it expands around the world. If your organisation is already established globally, we can build compliance reports to document the status of compliance with local laws and regulations and provide remediation plans and advice.

CANADA

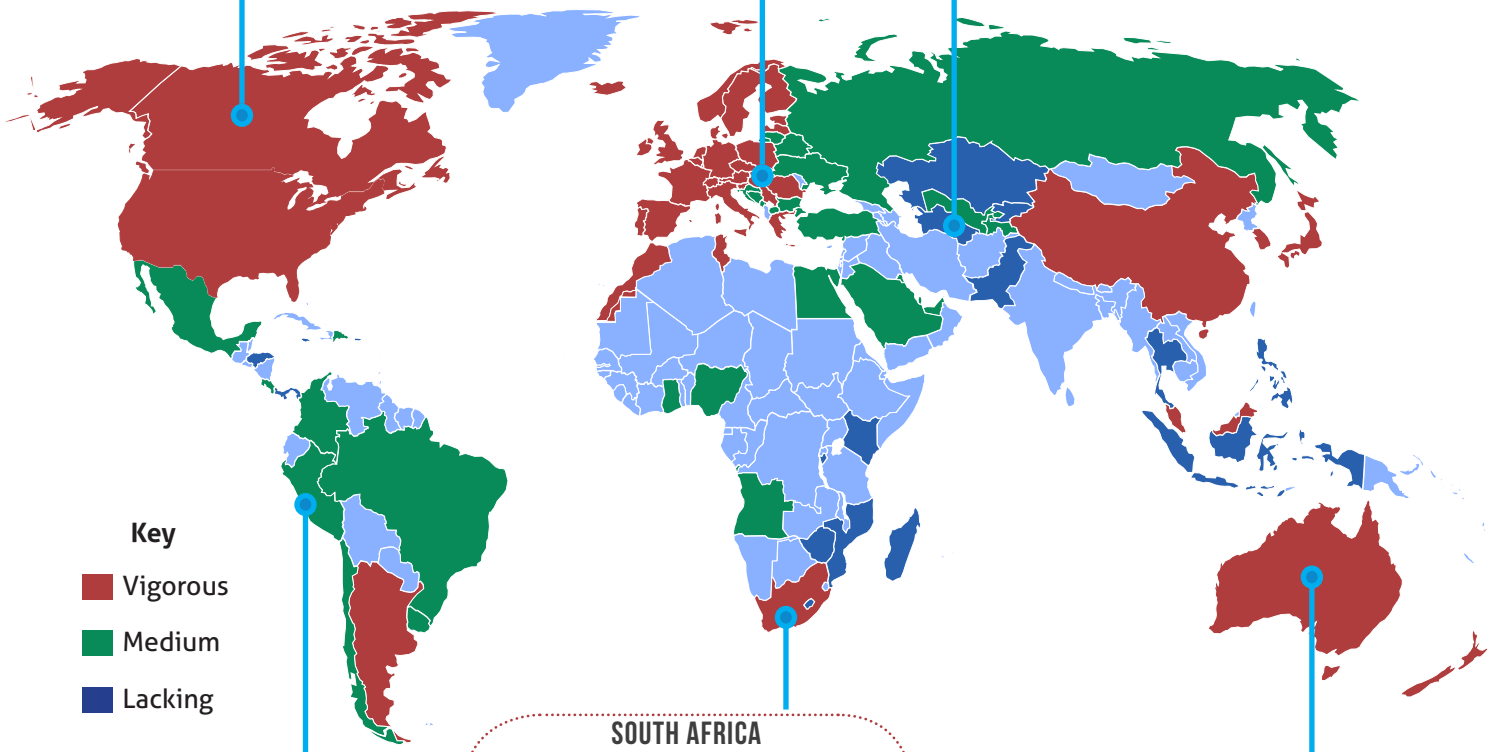
In April 2018, the Personal Information Protection and Electronic Documents Act aligned much of Canada's data protection legislation with the GDPR.

SLOVAKIA

While Slovakia is a member of the EU, its New Personal Data Protection Act of 2018 introduced a number of derogations from the GDPR, such as the possibility of publishing contact details of employees.

TURKMENISTAN

Turkmenistan introduced the principle of consent-based data collection, storage and processing into law in 2017, however no special office has been established to oversee the implementation of the statute.



PERU

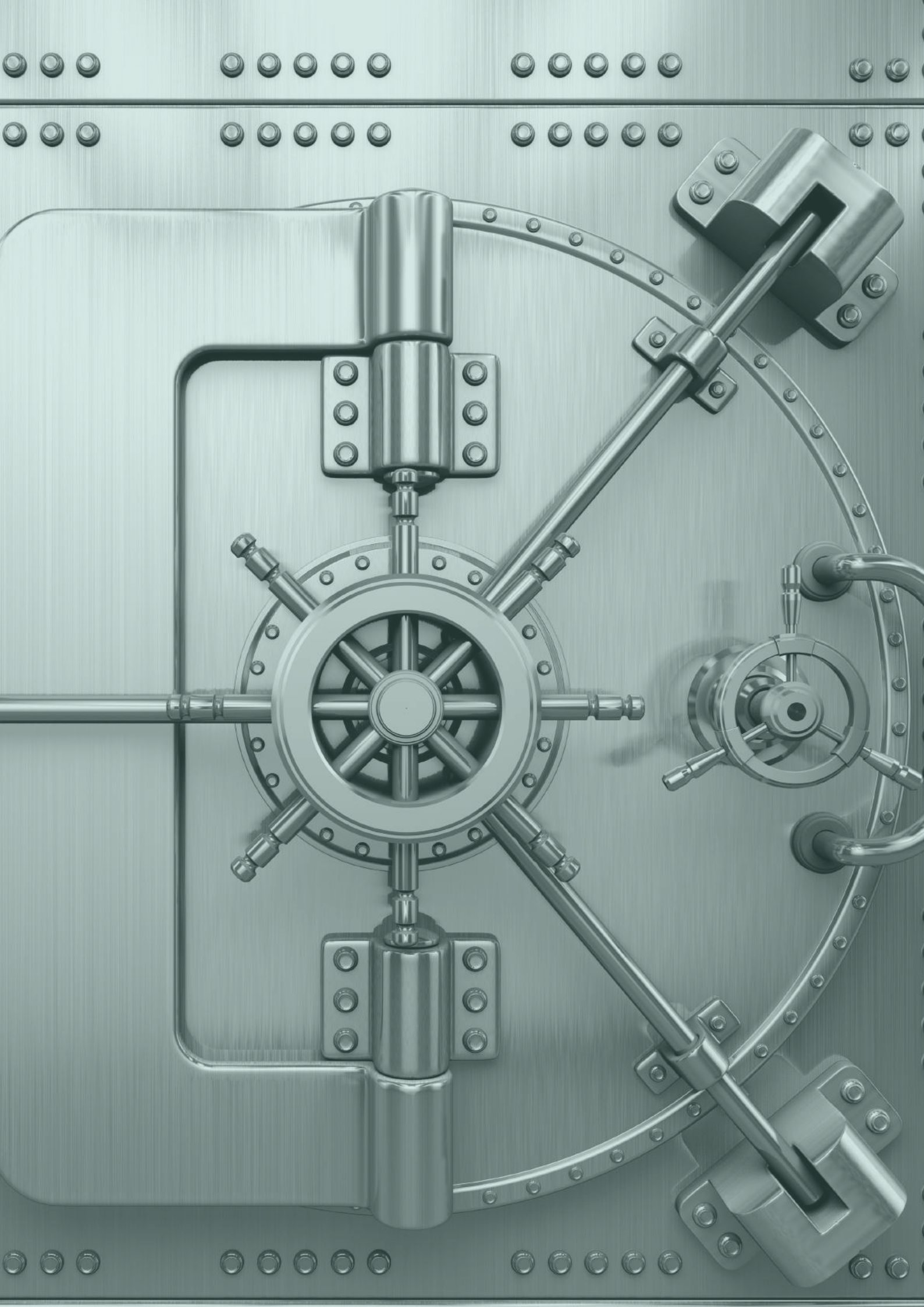
The National Authority for Personal Data Protection is Peru's equivalent to the ICO.

SOUTH AFRICA

The Information Regulator published the final POPI regulations on 14 December 2018. The purpose of the POPI Act is to ensure all South African institutions conduct themselves in a responsible manner when collecting, processing, storing and sharing personal information.

AUSTRALIA

Data Protection and Privacy law in Australia varies from state to state. In 2010, federal law introduced the right for individuals to request their data from third parties.



Data Protection Officer Support

We can support your Data Protection Officer or identified Data Protection Lead in ensuring appropriate compliance with the GDPR, DPA and related legislation

Under the GDPR, you must have a DPO if you are a public authority; carry out large-scale, regular and systematic monitoring of individuals; or process large levels of sensitive data. Even if you don't meet these criteria, it will still be essential to ensure you comply with data protection legislation and manage ongoing risks to personal information.

By either supporting your existing Data Protection Officer (DPO) or responsible lead, or by directly providing a DPO function, we can help you identify and mitigate against risks to personal information and ensure you continue to meet your legal obligations under data protection law. Our key areas of support include creation and implementation of improvement plans, policy and procedure review and development, records of processing and development and delivery of training and awareness programmes.

As every organisation will have different requirements in terms of levels of support needed, Evolve North will work with you to understand your needs and provide a bespoke solution based on your requirements.

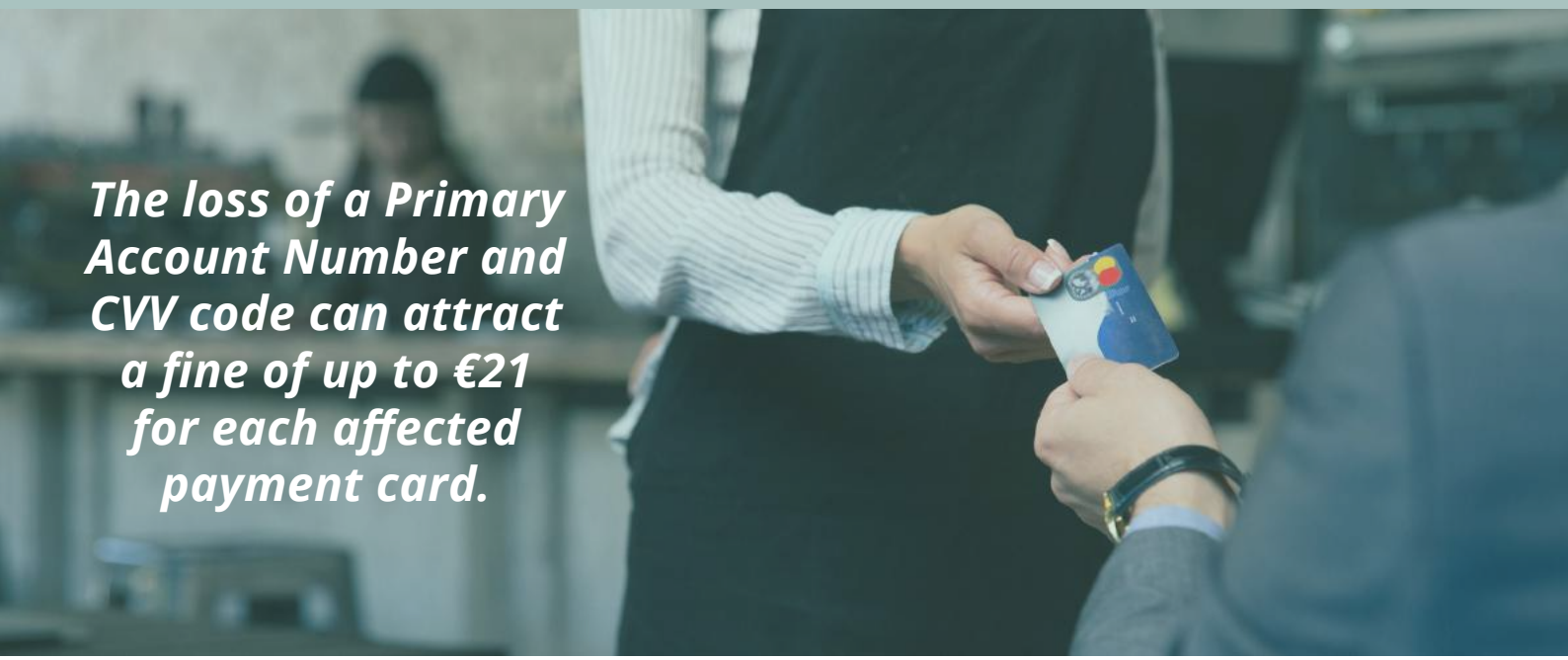
Our DPO support service at a glance...

- **Compliance Reviews**
  We'll identify gaps in your current compliance and provide ongoing auditing to ensure continued compliance with DP law.
- **Ongoing Support to help you Remediate**
  We'll guide you in implementing appropriate actions to remediate identified risks.
- **Responding to Key Events and Activities**
  You'll get advice and support for dealing with data breaches, managing data subject access requests or completing DPIAs.
- **Further Help and Advice**
  Our ongoing advice and guidance in relation to appropriate management of personal information will support continued compliance.

Data protection practitioners play a crucial role in ensuring that organisations' data protection practices are keeping up with changes in technology and truly putting people at the heart of what they do

Elizabeth Denham, Information Commissioner

[1]2017 Accenture Cybertech Europe



PCI DSS Support

We support our customers in meeting their PCI Data Security Standard obligations, supporting them through the process of completing the SAQ and becoming compliant

Understanding what you need to do to become compliant with the PCI DSS and signing off the Self-Assessment Questionnaire can be a daunting experience. Over the last decade, Evolve North have been helping organisations to navigate the process of reaching compliant status and maintaining that status year after year.

From the initial gap analysis process to the final sign-off of the SAQ, our certified PCI Professionals and data protection experts will provide guidance and help to ensure that all areas of the standard are met to deliver a successful outcome.

Our PCI DSS support service at a glance...

Gap Analysis
We'll review the Cardholder Data Environment and work with you to identify areas of remediation needed to become compliant.

Prioritised Approach Toolkit
We use a prioritised approach toolkit to help manage the path to compliance while providing quantifiable scoring and visibility of their progress as they implement new controls.

Implementing IT Security Controls
Support in understanding and implementing appropriate technical controls in line with requirements.

Support with Key Policies and Procedures
Development of key IT and IG policies and procedures that meet the requirements of the standard.

Cyber Essentials

The Cyber Essentials certification scheme is now a must-have for many UK businesses

Cyber Essentials provides you with a good understanding of where your organisation is positioned against an array of cyber threats.

Evolve North have extensive experience in guiding organisations through the Basic and Plus schemes to successfully obtain certification. This will save you time and optimise your ability to successfully demonstrate your commitment to protecting the information you hold.

Cyber Essentials Basic vs. Cyber Essentials Plus

	Cyber Essentials Basic	Cyber Essentials Plus
Description	Cyber Essentials Basic provides organisations of all sizes and in all sectors with a focused set of technical controls which will provide cost effective, basic cyber security protection from the most prevalent forms of threat coming from the internet.	Cyber Essentials Plus offers a natural progression from Cyber Essentials Basic. Cyber Essentials Plus offers a higher level of assurance of an organisation's cyber security defences through a range of internal and external tests of the organisations network and computers.
Coverage	• Policies and procedures	• Policies and procedures • External internet facing perimeter and services • Email and web gateways • User endpoints and mobile devices
Threats Replicated	• External internet-based attackers	• External internet-based attackers • Malicious users
On-site visit	No	Yes (some exceptions exist)
Cyber Insurance	£25,000 free cyber insurance for certified organisations	£25,000 free cyber insurance for certified organisations
Cost	£300 exc. VAT	Increased cost to cover on-site testing and accrediting body application fee
Badge		

ISO 27001

What is ISO 27001?

ISO 27001 is a globally recognised standard for implementing an Information Security Management Service (ISMS). The standard helps organisations keep information, such as financial information, intellectual property and employee details, secure by analysing and addressing information risks.

The ISMS contains a set of policies, procedures, technical and physical controls to protect the confidentiality, availability and integrity of information. It helps manage and keep secure information held by the organisation.

Implementing ISO 27001 improves organisational culture with regards to information security and ensures that future organisational and environmental changes do not introduce excess risk to the organisation.

Certified or Compliant?

Whether your organisation is looking to become certified or compliant will depend on the driving factor, usually this is a customer requirement.

The difference between Compliant and Certified is relatively simple. A compliant organisation has implemented an ISO 27001 ISMS in their organisation and has opted to self-certify this compliance. A certified organisation has had their ISMS audited by an ISO 27001 certification auditor who validates its compliance with the standard.

What does it cost?

Costs of implementing ISO 27001 vary for each organisation depending on the scope of the project.

We recommend you contact us for a discussion about the likely cost to your organisation.

We can help you to become ISO 27001 Certified or Compliant

evolvenorth

How can Evolve North help my organisation to implement ISO 27001?

Evolve North has a great deal of experience in supporting organisations to become ISO 27001 Certified or Compliant. Our team of professionals includes ISO 27001 Lead Auditors with many years' experience working in some of the most complex and demanding environments.

We can work with you to plan your organisation's Certification or Compliance roadmap by establishing the scope of your ISO 27001 implementation, developing a business case for the implementation and supporting you in the development and deployment of the ISMS and in attaining certification.

Our ISO 27001 support service at a glance...

Business Case
We'll gather information and calculate the benefits of ISO 27001, defining and agreeing stakeholder value and risk appetite and supporting your business case.

Implementing the Solution
By putting together a tailored plan for a phased and supported approach, we'll prepare your organisation for a successful ISMS deployment.

Getting Certified
Running the system and measuring its effectiveness against clear SMART (specific, measurable, achievable, realistic, timebound) objectives.

Continuous Improvement
Through a programme of audit, we will establish and document areas for continuous improvement.

NIS Directive

What is the NIS Directive?

The NIS Directive is designed to assist organisations in ensuring suitable technical and procedural controls are deployed within the organisation to prevent, manage and remediate cyber security risks and events for organisations that run and maintain National Infrastructure.

The EU has detailed the requirements of NIS by implementing the DSP Regulation, many of the requirements align with the GDPR.

Who is required to comply with the NIS Directive?

NIS applies to two groups of organisations: operators of essential services (OES), such as energy, transport, health and water; and relevant digital service providers (RDSPs), which include online search engines, online marketplaces and cloud computing services which have their head office in the UK or have nominated a UK representative, and have more than 50 staff and a turnover or balance sheet of more than €10 million.

The ICO can enforce NIS via enforcement notices, powers of inspection and penalties of up to £17 million for organisations which must comply but do not.

What are the requirements?

The NIS directive stipulates that organisations within the remit of NIS must "identify and take appropriate and proportionate measures to manage the risks posed to the security of a network and information systems", this includes:

- ensuring a level of security appropriate to the risk posed
- preventing and minimising the impact of incidents affecting digital services
- taking into account the requirements of the DSP Regulation

Evolve North can support you in ensuring you meet your NIS Directive obligations.

Our NIS Directive support service at a glance...

Gap Analysis
We'll identify where you do and don't comply with the directive, and provide you with easy to follow remediation tasks.

Remediation
We can offer hands-on technical and governance support in remediating to comply with the NIS Directive.

Support Documents
We have a range of support documentation including Policies and Procedures which we can tailor to your organisation's needs.

Support with Key Policies and Procedures
Development of key IT and IG policies and procedures that meet the requirements of the standard.

evolve north

Evolve North translate the boring stuff into actions that make more sense.

IT Manager, Newcastle International Airport

Privacy and Electronic Communications Regulation

We can help your organisation understand the implications of current privacy law on your marketing practices and other impacts of the Privacy and Electronic Communications Regulations (PECR)

PECR should be considered alongside the Data Protection Act, in relation to specific types of data processing. These include where you are using personal information to carry out direct marketing, if you're using certain types of cookies on your websites and potentially if you provide a function that allows someone to look up contact details of individuals on a directory. In addition there are further requirements for electronic communications service providers.

Evolve North can help you consider where your current promotional activities would be classed as direct marketing, making sure you're carrying out marketing in line with current privacy law. This will include considering whether or not you need consent from individuals, which may be influenced by your marketing approach and who you're targeting. We can also help you understand whether you can continue to use your marketing lists in the same way and any implications of bought in lists.

We also help organisations understand the types of cookies they use currently, whether a cookie notice may be required on websites and help you develop cookies policies that effectively inform website users about how their data is used and their options for not sharing information via cookies.

Our PECR support service at a glance...

- **Documentation and Analysis**
  We'll review your current practices around appropriate marketing and use of electronic communications.
- **Ongoing Remedial Support**
  We'll provide guidance on where further improvements may be needed and help to implement these improvements.
- **Review of Website Compliance**
  Reviewing your current websites will allow us to ensure you are compliant with PECR and the GDPR.
- **Training**
  Regular training of staff or key groups on the implications of PECR, DPA and the GDPR will ensure a culture of awareness in the organisation.

New ePrivacy Regulation

PECR is based on the 2002 EU ePrivacy Directive, but a new ePrivacy Regulation is currently being finalised and will work alongside GDPR in the future. This could have an impact on how you currently carry out marketing or more generally on electronic communications in your business. Evolve North can help you consider the impact of these new regulations as they are implemented.

Phone. 01748 905 002
Email. info@evolvenorth.com

Evolve North have a good insight of how the NHS operates and some of the challenges that can bring.

IT Team Leader
Health Education England

Data Security and Protection Toolkit

We provide help and guidance to health and social care organisations implementing the Data Security and Protection Toolkit

The NHS Digital Data Security & Protection Toolkit allows organisations that process health and social care data to demonstrate their compliance with Data Protection Law and the National Data Guardian Data Security Standards. It will be used by the Care Quality Commission to monitor best practice.

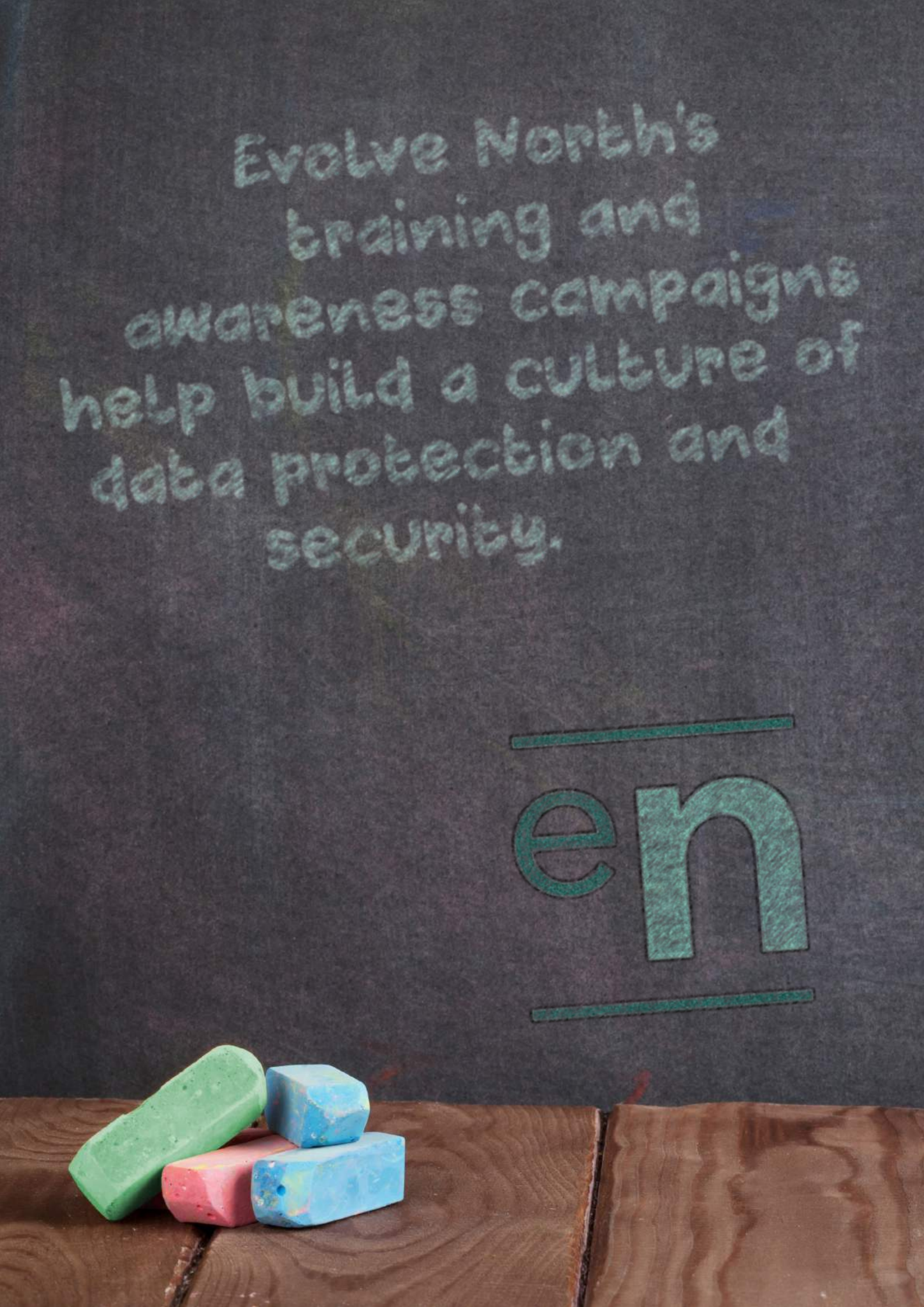
We can support you in fulfilling the requirements of the DS&P Toolkit in a number of ways. This may include carrying out an independent audit of your current evidence to identify areas where further work may be needed or helping to fill gaps in current areas of compliance, such as identifying and recording your information assets, risk assessing these assets, ensuring appropriate reviews of third parties are being carried out, helping train your staff or developing new policy, procedure and guidance documents.

Evolve North's mix of governance and data security expertise and extensive experience of working with health and social care organisations makes us ideally placed to support your needs in this area.

Our DS&P service at a glance...

- **Toolkit Completion**
  We'll work with you to complete the toolkit and identify areas where further work may be needed to reach compliance.

- **Policies and Procedures**
  Our consultants will develop IG policies and procedures and roll out training and awareness campaigns.


Evolve North's
training and
awareness campaigns
help build a culture of
data protection and
security.

Building a Training and Awareness Approach

We can help organisations understand the training requirements of their organisation and roll out effective Data Protection and IT Security training

Your staff need to understand what information they need to protect, why it's important to protect it and how they can do this. By training staff you will be protecting both them and your organisation from the detrimental effect of a data breach which may involve damage to your reputation, potential financial loss and possible fines from the ICO.

We can work with you to identify the training requirements of different staff groups, help you construct an effective training and awareness campaign and deliver training to staff via face to face or online sessions.

Our consultants will work with you to fully understand the purpose of the training and the intended audience so that an approach to training and awareness raising can be developed which is tailored to your organisational needs. We can help you ensure that staff at all levels understand how effective management of personal data can protect both them and your organisation.

Our training and awareness service at a glance...

- **Planning**
  We'll work with key leads to develop a training and awareness campaign that meets the needs of your business.

- **Raising Awareness**
  Our consultants will identify materials and methods that will best raise awareness of potential risks to confidential information.

- **Training Delivery**
  We'll provide face to face or remote training sessions to your staff at a time and location that suits your needs.

- **Monitoring**
  We'll identify the most effective methods of monitoring staff training completion and testing staff understanding.

Sophos Services and Solutions

Sophos endpoint, encryption, web, email, mobile and network security solutions simplify security to protect your business and help you meet compliance needs.

It takes a lot more than antivirus to cover every threat to your business. At Evolve North, we are well-versed in the complexities of data security. We can assist you in all aspects, from technology through training, business changes, strategies, policies and procedures.

We are Sophos Certified Architects and here to help you get the most from your Sophos products. Email us for a free, no-obligation consultation.

XG Firewall

Sophos XG Firewall provides comprehensive next-generation firewall protection that blocks unknown threats, automatically responds to incidents, and exposes hidden risks.

Sophos UTM

Unified Threat Management makes security simple. Sophos UTM provides the ultimate network security package with everything you need in a single modular appliance.

Web Security Appliance

Advanced web protection made simple. Sophos' purpose-built secure web gateway appliance makes web protection simple. It provides advanced protection from today's sophisticated web malware with lightning performance that won't slow users down.

Safeguard Encryption

SafeGuard Encryption has the ability to intelligently protect your data against theft. It automatically encrypts your content, and the content stays encrypted even when it's shared or uploaded to a cloud-based, file-sharing system.

Email Security Appliance

The majority of ransomware is contained in malicious emails. Advanced email security and control made simple. Sophos' purpose-built secure email gateway is an all-in-one solution for email encryption, DLP, anti-spam and threat protection.

Endpoint Protection

Sophisticated yet simple security for your desktop environment. Sophos Endpoint Protection makes it simple to secure your Windows, Mac and Linux systems against malware and advanced threats, such as targeted attacks.

Sophos Authorised Training Centre

As a Sophos Authorised Training Centre, we are certified to run customer training classes on behalf of Sophos.

Sophos Administrator courses are designed to help you get the most from your Sophos products and investment. You'll have the opportunity to learn about the full range of features, and how you can harness these to get the most out of your product and ensure you have the skills and knowledge required to protect your organisation from the latest threats,

Courses cover:

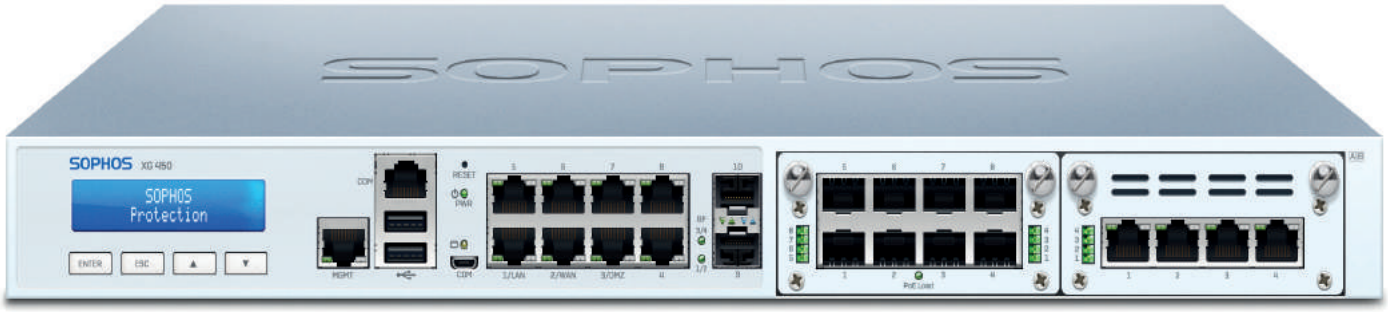
- Configuration
- Responding to and managing security events
- Analysing logs and reporting
- Troubleshooting
- Day-to-day tasks
- Backup, restore and recovery

Correctly configured and maintained products also assist in meeting your regulatory compliance requirements.

Training Schedule

We run regular training courses throughout the year across the North of England and Scotland on all Sophos products, including Sophos Central, Sophos Endpoint on-premises and Sophos SafeGuard. Check our website for an up-to-date schedule.

Training courses can also be delivered privately at your premises and we welcome you to contact us to discuss your requirements.



I found Evolve North easy to work with and knowledgeable in all areas of compliance from PCI DSS to Data Protection

Compliance Manager
Village Group

evolve north

Identity and Access Management

Improve security and take the burden of identity provisioning and deprovisioning out of IT's hands

A carefully designed and implemented Identity and Access Management (IDAM) solution enhances security, compliance and efficiency across your IT landscape. We have a great deal of experience in designing and implementing IDAM solutions, incorporating role-based access control and privileged access management.

Working closely with stakeholders across the business, we'll scope and document the target automated identity landscape, ensuring IT and Governance requirements are met. Our solutions connect authoritative sources, such as HR databases, to downstream systems, such as Active Directory and other third party applications and cloud-based applications.

A comprehensive IDAM solution will ensure: users only get access to the information they need to do their job; user joiner, mover and leaver (JML) processes are automated and performed quickly; users only have one identity across all applications with consistent attributes based on a single source of information.

Our Identity and Access Management services at a glance...

Scoping and Design
We'll talk to stakeholders in your business to establish the required lifecycles of identities based on IT, Governance and corporate requirements.

Ongoing Support
Support is available in the form of a support contract or as a managed service. We're here to help if you have future troubleshooting or change requirements.

Implementation
Working with you, we'll deploy an automated IDAM system to replace your existing JML process and

Training
We can provide knowledge transfer and support to your staff throughout the design, development and deployment of your IDAM solution.

Microsoft 365 Compliance Tools

We can help you get the most from your Microsoft 365 subscription on your journey to GDPR compliance

An ideal starting point is a detailed assessment of your GDPR readiness. We'll work with you to evaluate your organisation's privacy posture, uncover risks, provide expert guidance around the GDPR and offer recommendations specific to your organisation

Our approach

1. ***Discover***
   Discover what personal data you have and where it resides.
2. ***Manage***
   Manage how discovered personal data is used and accessed.
3. ***Protect***
   Establish security controls to prevent, detect and respond to vulnerabilities and data breaches.
4. ***Report***
   Keep required documentation, manage data requests and breach notifications.

We have the skilled personnel, process knowledge and Microsoft technology expertise to evaluate your current status and help you on your path to becoming compliant.

Evolve North were able to assess compliance readiness in a friendly open manner and provide reassurance to stakeholders.

Head of Technology
Linc Cymru Housing Association

Microsoft technology forms the basis of our GDPR solution

Process all in one place

Centralise processing in a single system, simplifying data management, governance, classification and oversight.

Maximize your protections

Protect data with industry-leading encryption and security technology that's always up-to-date and assessed by experts.

Streamline your compliance

Utilise services that already comply with complex, internationally-recognised standards to more easily meet new requirements, such as facilitating the requests of data subjects.

We will work with you to uncover risk and take action

Discover data across systems

- Discover and catalogue data sources
- Increase visibility with auditing capabilities
- Identify where personal information resides across devices, apps and platforms

Govern access and processing

- Enforce usage policies and access controls across your systems
- Classify data for simplified compliance
- Respond to data requests and transparency requirements

Protect through the entire lifecycle

- Protect user credentials with risk-based conditional access
- Safeguard data with built-in encryption technologies
- Rapidly respond to intrusions with built-in controls to detect and respond to data breaches

Penetration Testing

Penetration testing identifies risks in your IT environment

A penetration test forms part of a cost-effective risk mitigation plan, giving your customers assurance that you take IT security seriously by helping you to reveal and fix the vulnerabilities you didn't know existed before a hacker has a chance to find and exploit them.

Whatever your driving factor, be it a customer requirement, compliance requirement, or simply for your own satisfaction, we'll work with you to assess your application or network for vulnerabilities and weaknesses, delivering a detailed report of our findings.

Our penetration test reports provide details of discovered security issues and their risk to your organisation as well as remedial advice for each vulnerability found.

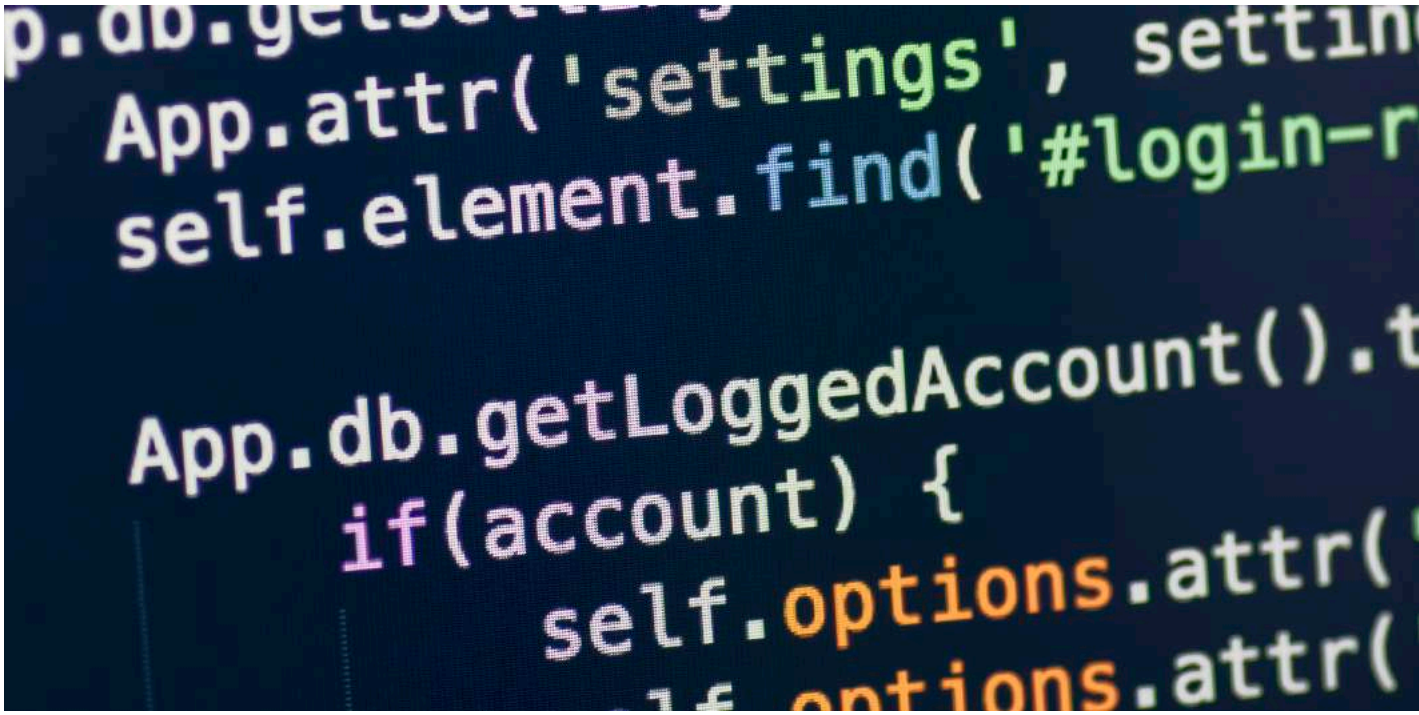
Our Penetration Testing service at a glance...

Assessment

Our penetration testers can assess your infrastructure, applications, mobile applications, wireless networks, physical security and more...

Ongoing Remedial Support

We'll provide guidance on where further improvements may be needed and help to implement these improvements.



Vulnerability Scanning

Regular vulnerability scans help you to detect and remediate the vulnerabilities in your environment before attackers can exploit them

The GDPR mandates that you have suitable processes in place to detect and report data breach. Vulnerability scanning is a proactive tool that ensures any external vulnerabilities are identified and reported in a timely manner to assist in your GDPR compliance.

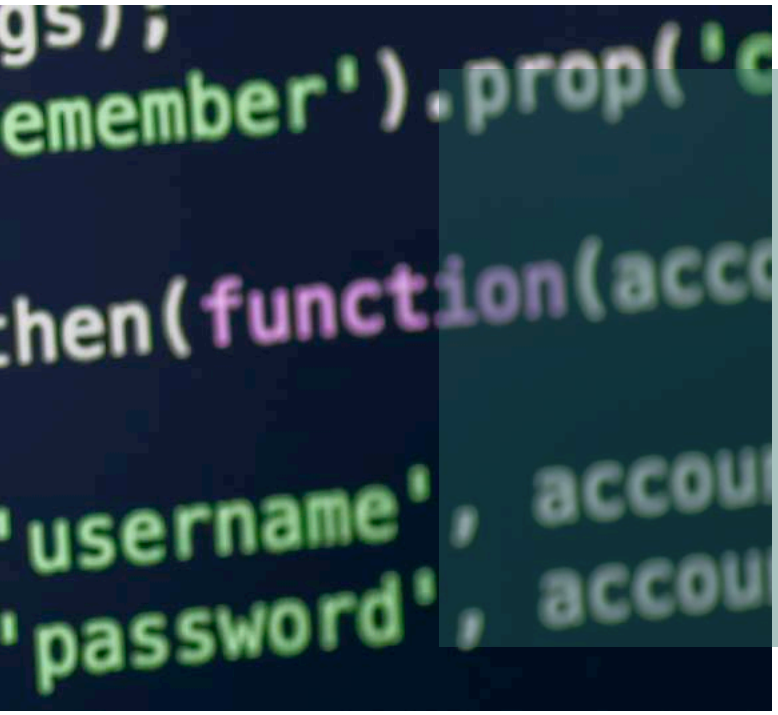
Our Vulnerability Scanning service gives you a hacker's view of your organisation's external IT infrastructure by regularly scanning for, and identifying, the known vulnerabilities that are present.

Use the vulnerability scan report to create your remediation plan and plug any security holes before hackers have a chance to manipulate them, saving you from financial and reputational damage.

Our Vulnerability Scanning service at a glance...

Pricing
Our quarterly vulnerability scanning service starts at just £495 for up to 10 IP addresses or domains.

Ongoing Remedial Support
We'll provide guidance on where further improvements may be needed and help to implement these improvements.



Vulnerability Scanning vs. Penetration Testing

Vulnerability scans and penetration tests are very different from each other.

Vulnerability scans automatically search systems for known vulnerabilities and are a low cost and effective means of validating security.

Penetration tests attempt to exploit weaknesses in a network or application and are a more manual and time consuming process yielding more detailed results.

Phishing Simulations and Training

Determine the level of risk a phishing attack poses to your organisation by performing a simulated attack

93% of social attacks are phishing related.[1] A phishing simulation helps to increase employee awareness and decrease the likelihood of a successful phishing attack against your organisation.

The results of a phishing simulation can be used to determine both the level of risk a phishing attack would pose to your business, and the education requirements of your users.

We can work with you to tailor a phishing campaign, or campaigns, that incorporate simulated phishing attacks, user education and fully documented reports and remedial guidance.

Our Phishing Simulation service at a glance...

Documentation
We'll document the results of your simulation and present as PDFs, with supplementary Excel spreadsheets.

One-off or Regular Simulations
We can provide one-off or regular campaigns which provide results comparisons and allow you to track campaign effectiveness.

Guidance to Help You Remediate
Remedial advice is provided, and bespoke training may be delivered to complement the simulations.

Training and Awareness
We can provide staff training in the form of computer-based training or on-site classroom-based training.

Do your users reuse passwords?

Believe it or not, it is estimated that 73% of online accounts are guarded by duplicate passwords with 54% of people using fewer than 5 passwords across their entire online life.[2]

A campaign of training and awareness and auditing can help your users choose strong passwords and ensure they understand the risks present when reusing passwords.

1. Data Breach Investigations Report, Verizon
2. Password Statistics: The Bad, the Worse and the Ugly, Entrepreneur Europe

Password Auditing

Password auditing helps you to eliminate weak passwords from your IT environment and to ensure you have a password policy that works

A regular password audit will test that your password policy is effective and that your users are setting strong passwords. Strong passwords are necessary to avoid breaches and secure your data.

Password auditing, combined with user education, is also an effective way of motivating users to set complex passwords by demonstrating how quickly and easily weak passwords can be cracked.

Our password audits can be tailored to your exact requirements. With advanced results reporting, IT administrators are able to drill down and identify precisely where the highest risks to the organisation exist, meaning remedial activities can be highly targeted.

Our Password Auditing service at a glance...

Documentation
The results of your audit will be documented with key areas of risk, such as cracked privileged accounts, highlighted for your convenience.

Guidance to Help You Remediate
Our documentation includes recommended password policy wording to help you ensure your users are setting strong passwords.

Regular Auditing
We recommend bi-annual auditing be performed and we can compare your latest results with historical results to track campaign effectiveness.

Training and Awareness
We can provide staff training in the form of computer-based training or on-site classroom-based training.

[1]2018 Hiscox Small Business Guide to Cyber Attacks
[2]2017 Verizon Data Breach Investigations Report

The superior man, when resting in safety, does not forget that danger may come. When in a state of security he does not forget the possibility of ruin. When all is orderly, he does not forget that disorder may come. Thus his person is not endangered, and his States and all their clans are preserved.

Confucius