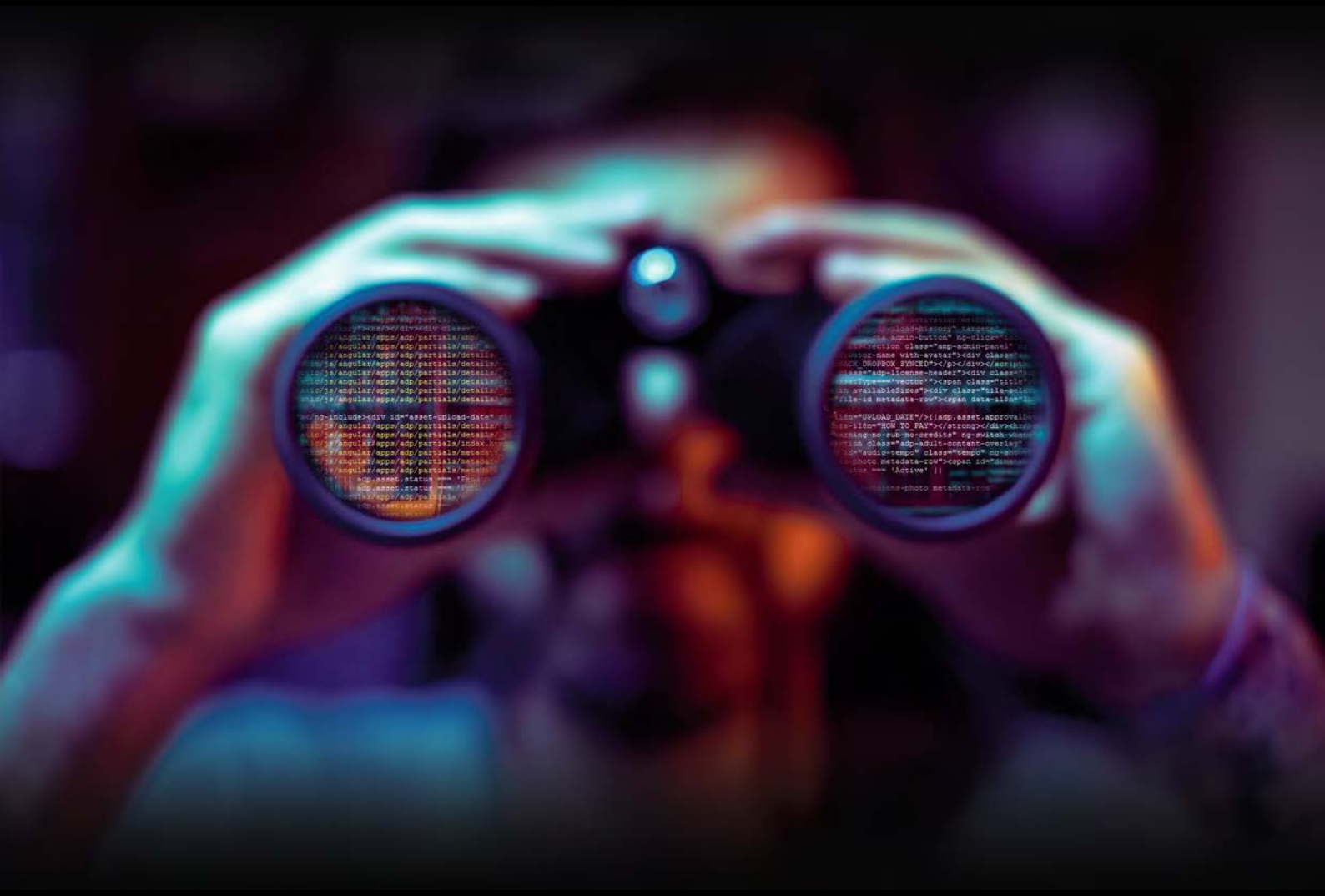
bsi.

...making excellence a habit.™



understanding your CYBERSECURITY RISK

How standards can help you protect your organization

Understanding your cybersecurity risk

Cybersecurity is an issue for every organization across the world, regardless of size or focus. Over the past decade it has moved from a technical specialism to a mainstream concern for individuals, businesses and government.

Despite this, many organizations are still not doing enough to protect themselves. According to a 2019 cybersecurity study conducted by IBM, which surveyed more than 3,600 security and IT professionals from around the world, three-quarters of businesses do not have a plan in place to respond to a cybersecurity incident.

Also, a significant proportion (45%) of companies that do have such a process in place don't test it regularly, or even at all, making it impossible to keep up to date and exposing vulnerabilities in a fast-moving environment. This is no longer just an issue for IT professionals – in today's world, all organizations and their employees must take responsibility for digital security.

From the biggest government department shielding critical infrastructure 24 hours a day, to a microbusiness looking after its customer data, the right awareness and knowledge is needed to guide everyone in the workplace.

The most effective way to improve cybersecurity is by using internationally recognized standards to introduce processes which protect against both deliberate and chance incidents.

Standards help companies improve their cybersecurity levels in a number of ways – from informing new processes to shield your company to delivering more effective employee training, as well as introducing better data protection and assisting with legislative compliance.

So, what are the key areas of cybersecurity risk for most companies, and which standards can help organizations address them?

Data privacy

Every organization, public or private, runs on data – its own and that relating to its employees and partners, as well as customer or user data.

With new information generated every second, it's imperative to stay in control of how it's stored, who can access it and how it's managed.

Also, with GDPR now firmly in place, the financial consequences for a significant data breach are very serious – not to mention the potential reputational damage.

Businesses can use ISO/IEC 27001 to implement an overarching information security management system, while ISO/IEC 27701 focuses on improved privacy controls.

Cloud security

Cloud computing is another area which has transformed the way that most organizations store data, in just a few years.

Although many businesses initially felt cautious about transferring critical data and functionality to the cloud, it has now become commonplace, with standards playing a key supportive role.

There are a number of standards that help organizations make the right choices when selecting cloud service providers, and then control the resulting storage arrangements.

One of the most relevant is ISO/IEC 27017:2015 which outlines guidelines for information security controls around the provision and use of cloud services – covering implementation as well as management processes.

PROTECTION AGAINST CYBERASSAULTS

BS 31111

Cyber risk and resilience. Guidance for the governing body and executive management

ISO/IEC 27032

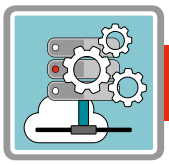
Information technology – Security techniques – Guidelines for cybersecurity

ISO/IEC 27033

Information technology – Security techniques – Network security

ISO/IEC 27034

Information technology – Security techniques – Application security



DATA MANAGEMENT AND CLOUD STORAGE

ISO/IEC 27701

Privacy Information Management – Security techniques. Extension to ISO/IEC 27001 and ISO/IEC 27002. Requirements.

ISO/IEC 27017

Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services

PROTECTING COMPANY INFORMATION

ISO/IEC 27001

Information technology – Security techniques – Information security management systems – Requirements

ISO/IEC 27002

Information technology – Security techniques – Code of practice for information security controls

ISO/IEC 27003

Information technology – Security techniques – Information security management system implementation guidance

ISO/IEC 27005

Information technology - Security techniques - Information security risk management

BS 7799-3

Information security management systems. Guidelines for information security risk management

Bring your own device (BYOD)

With the rise of flexible and home-based working, many more employees are working remotely as opposed to gathering in a single location.

A lot of companies use a bring your own device (BYOD) system which sees staff using personal mobile devices for work activities. Although this can improve efficiency it also adds a layer of risk, since these devices are connected to corporate networks.

Employee awareness and understanding of BYOD security responsibilities are critical to organizational risk.

Creating a clear policy for all staff, in line with ISO/IEC 27001 requirements, is the best way to mitigate security risks associated with BYOD arrangements. We also recommend referring to BS ISO/IEC 38500, which provides guidance for IT governance.

Human error

Recent research puts human error as the top cause of cybersecurity incidents.

Criminals know to exploit individuals, rather than systems, because they understand just how vulnerable busy, distracted people can be – especially those who might not have cybersecurity front of mind.

However, standards put security-awareness training at the forefront to help strengthen your cybersecurity chain, empowering employees to become a 'human firewall'. Using phishing simulations and knowledge assessment, organizations can accurately assess specific training requirements, and current risk – ideally at the individual user level.

Using this as a baseline, companies should then tailor plans to an employee's needs. The information security standard ISO/IEC 27001 helps companies create and structure training in accordance with international best practices, as well as define responsibilities and protocols in the event of a breach.

You can get individual copies of every standard in our shop, or access and manage your collection of cybersecurity standards packages using British Standards Online (BSOL).

bsi. BSOL
Standards Online

The reassuringly easy way to work with standards

BSOL is a simple online tool that gives you instant access to the standards you need, making life a lot easier. It's easy to build your own database of relevant standards. Then you can find what you need fast and stay right up to date – so you can avoid costly errors and work with confidence.

Know you're covered

Save time
Manage all your standards in one place. You can access ISO, EN, BS ASTM and IEC standards through BSOL – and it takes only seconds to search.

Save money
Make standards even better value for money. Using BSOL gives you large savings on your traditional standards spend.

Miss nothing
Get an alert whenever a standard changes and understand the significance immediately. Then view the differences to key standards, so you can track exactly how they've changed.

Reduce risk
Track past, present and future changes. With access to historic and emerging standards, you can see the guidance that informed previous decisions, as well as changes that could shape your future moves.

Fit the way you work

Tailored to you
Subscribe only to the standards you need, use pre-built modules or build personal collections.

Full flexibility
You can still access every standard in the system and update your choices at any time.

Easy monitoring
Monitor which standards your users are working with, and easily spot gaps or overlaps.

Free and unlimited training
Our training team are here to give you extra support if you need it.

Make life easier with BSOL.

Get a quote or find out more at bsigroup.com/bsol.
Or call +44 (0)345 086 9001.

bsi.

...making excellence a habit.™

UNDERSTANDING YOUR CYBERSECURITY RISK

Key Cybersecurity Standards

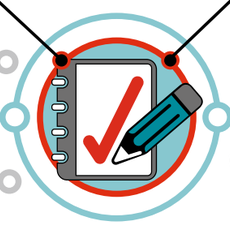
ISO/IEC 27701
Privacy Information Management – Security techniques. Extension to ISO/IEC 27001 and ISO/IEC 27002. Requirements.

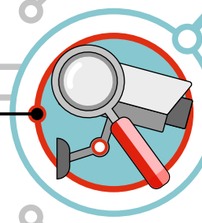
BS 31111
Cyber risk and resilience. Guidance for the governing body and executive management.

ISO/IEC 27032
Information technology – Security techniques – Guidelines for cybersecurity.

ISO/IEC 27002
Information technology – Security techniques – Code of practice for information security controls.

ISO/IEC 27003
Information technology – Security techniques – Information security management system implementation guidance.





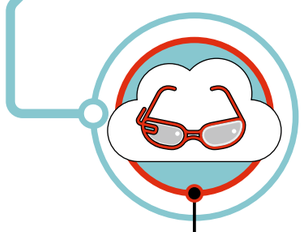
DATA MANAGEMENT AND CLOUD STORAGE

PROTECTION AGAINST CYBERASSUALTS

PROTECTING COMPANY INFORMATION

ISO/IEC 27001
Information technology – Security techniques – Information security management systems – Requirements.

ISO/IEC 27034
Information technology – Security techniques – Application security.



ISO/IEC 27033
Information technology – Security techniques – Network security.

ISO/IEC 27017
Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services.

ISO/IEC 27005
Information technology – Security techniques – Information security risk management.

BS 7799-3
Information security management systems. Guidelines for information security risk management.

bsi.

...making excellence a habit.™

cloud services ASSURANCE

How standards can help you select and manage cloud service partners

Cloud services assurance

The acceleration of high-speed wireless internet connection, coupled with advances in processing technology, has led to the proliferation of data across all sectors — and for organizations of all sizes.

At the same time increases in cyber risk, and rising uncertainties around information security, has meant that the way data is managed and stored has become a board-level issue. This unprecedented growth in data volumes has redefined how business is run, with cloud computing transforming the way organizations store data.

Although many initially felt cautious about transferring critical information and functionality to the cloud, it has now become commonplace and offers significant access and cost-saving advantages.

Adopting cloud technologies

At a time where investments and the ongoing resource that is being dedicated to data protection, it's unsurprising to see businesses and governments alike adopting cloud-based technologies, in the understanding that a well-chosen service is the most secure option available. Plus, with the right controls in place, cloud storage can reduce both vulnerability to human error and deliberate insider sabotage, making it an even more attractive proposition.

Where there is still hesitation or uncertainty on cloud adoption, standards can help organizations to make the right choices when selecting cloud service providers, as well as govern their ongoing storage arrangements and assist with associated regulatory compliance.

Managing cloud service relationships

When it comes to managing ongoing relationships, establishing clear roles and responsibilities is important. Generally, the cloud services provider handles the hardware, operating system, platform and application security.

This third-party company will ensure that the customer's data is stored confidentially and can't be changed, while maintaining the correct availability to those who need to access it. Businesses using this service remain responsible for assigning employees to the right roles and controlling access and permissions.

How you categorize cloud service data also requires collaboration between parties. From what the user of cloud services submits or creates to the data the cloud storage provider needs to run the service effectively. Plus, how is derived data – things that the provider can observe from the customer's use of the cloud service – defined? And what about data relating to the working relationship?

All these questions need consideration and standards like ISO/IEC 19944 (data flow, data categories and data use in the cloud) can help. The standard also provides a structure for making statements about how data will be used by the provider. This can be used in legal service agreements, and to ensure transparency between the two parties. Seeking out the right quality and process assurances from potential service providers is critical.

Key Cloud Services Standards

PROTECTING COMPANY INFORMATION

ISO/IEC 27000

Information technology — Security techniques — Information security management systems — Overview and vocabulary

ISO/IEC 27001

Information technology – Security techniques – Information security management systems – Requirements

ISO/IEC 27002

Information technology – Security techniques – Code of practice for information security controls

ISO/IEC 27003

Information technology – Security techniques – Information security management system implementation guidance

ISO/IEC 27005

Information technology – Security techniques – Information security risk management

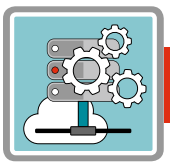
BS 7799-3

Information security management systems – Guidelines for information security risk management

PROTECTION AGAINST CYBERASSAULTS

ISO/IEC 27032

Information technology – Security techniques – Guidelines for cybersecurity



DATA MANAGEMENT AND CLOUD STORAGE

ISO/IEC 27017

Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services

ISO/IEC 27018

Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

ISO/IEC 27701

Privacy Information Management – Security techniques. Extension to ISO/IEC 27001 and ISO/IEC 27002. Requirements.

BS ISO/IEC 19944

Information technology – Cloud computing – Cloud services and devices Data flow, data categories and data use

Using standards to deliver cloud assurance

To enhance the way the customer organization works with the cloud provider, ISO/IEC 27017 specifies information security controls for cloud services, including clarification on both parties' roles and responsibilities to help make cloud services safe and secure. This is just one of a family of standards dedicated to giving assurance around information and data security.

ISO/IEC 27018 provides a code of conduct for handling personally identifiable information – particularly helpful in light of stringent privacy regulations such as the general data protection regulation (GDPR), and similar international legislation. Standards development in this area is also very active — ISO/IEC 27701 delivers an extension to the ISO/IEC 27000 series focusing on privacy information management.

All these standards come from the ISO/IEC 27000 family focused on information security, cybersecurity and privacy management. The series provides an overview and introduces important terminology for an information security management system (ISMS), while ISO/IEC 27001 defines key requirements. ISO/IEC 27002 outlines codes of practice and specific controls (including cloud services) and ISO/IEC 27003 helps organizations implement their ISMS.

In addition to all this, BS 7799-3 provides further implementation support and guidance. Other relevant standards include ISO/IEC 27032 which gives guidance on cybersecurity management, and ISO/IEC 27005 which outlines techniques for information security risk management. Both support organizations in protecting themselves against accidental or deliberate incidents.

All these standards provide best practice knowledge and can help build organizational resilience, reducing the likelihood of data breaches, as well as the resulting impact if they do occur.

Summary

Given that data is one of the most important business assets, now most commonly stored in the cloud, international standards relating to information security and privacy management play a key role in governance.

They help companies optimize all related decisions and planning to maximize this asset in a secure, compliant way. With the right standards in place, businesses can provide greater reassurance to customers and stakeholders that this data is well protected, enhancing brand reputation and optimizing efficiency ●

bsi. BSOL
Standards Online

The reassuringly easy way to work with standards

BSOL is a simple online tool that gives you instant access to the standards you need, making life a lot easier. It's easy to build your own database of relevant standards. Then you can find what you need fast and stay right up to date – so you can avoid costly errors and work with confidence.

Know you're covered

Save time
Manage all your standards in one place. You can access ISO, EN, BS ASTM and IEC standards through BSOL – and it takes only seconds to search.

Save money
Make standards even better value for money. Using BSOL gives you large savings on your traditional standards spend.

Miss nothing
Get an alert whenever a standard changes and understand the significance immediately. Then view the differences to key standards, so you can track exactly how they've changed.

Reduce risk
Track past, present and future changes. With access to historic and emerging standards, you can see the guidance that informed previous decisions, as well as changes that could shape your future moves.

Fit the way you work

Tailored to you
Subscribe only to the standards you need, use pre-built modules or build personal collections.

Full flexibility
You can still access every standard in the system and update your choices at any time.

Easy monitoring
Monitor which standards your users are working with, and easily spot gaps or overlaps.

Free and unlimited training
Our training team are here to give you extra support if you need it.

Make life easier with BSOL.

Get a quote or find out more at bsigroup.com/bsol.
Or call +44 (0)345 086 9001.

bsi.

...making excellence a habit.™

CLOUD SERVICES ASSURANCE

Key Cloud Services Standards

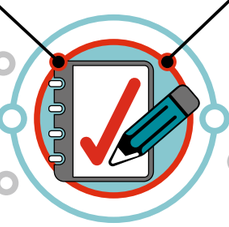
ISO/IEC 27701
Privacy Information Management – Security techniques. Extension to ISO/IEC 27001 and ISO/IEC 27002. Requirements.

BS ISO/IEC 19944
Information technology – Cloud computing – Cloud services and devices data flow, data categories and data use.

ISO/IEC 27032
Information technology – Security techniques – Guidelines for cybersecurity.

ISO/IEC 27002
Information technology – Security techniques – Code of practice for information security controls.

ISO/IEC 27003
Information technology – Security techniques – Information security management system implementation guidance.



DATA MANAGEMENT AND CLOUD STORAGE

PROTECTION AGAINST CYBERASSUALTS

PROTECTING COMPANY INFORMATION

ISO/IEC 27000
Information technology – Security techniques – Information security management systems – Overview and vocabulary.

ISO/IEC 27001
Information technology – Security techniques – Information security management systems – Requirements.

ISO/IEC 27017
Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services.

ISO/IEC 27018
Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.

ISO/IEC 27005
Information technology – Security techniques – Information security risk management.

BS 7799-3
Information security management systems. Guidelines for information security risk management.

bsi.

...making excellence a habit.™

managing data with CONFIDENCE

How standards can help you stay in control of data storage, access security and management processes

Managing Data with Confidence

Every organization runs on data. Information that it generates internally, receives externally, and stores for the short or long-term. This data can relate to its own operations, its employees and partners, and its customers or users. Tim McGarr, Sector Lead (Digital) at BSI explains how standards can help businesses stay in control.

With new information generated continually, it's imperative to stay in control of data storage, access security and management processes. Also, with the GDPR now firmly in place, the financial consequences of a significant data breach are very serious – not to mention the reputational damage a high profile incident can cause.

Surprisingly, given what's at stake, a 2019 IBM cybersecurity study of global security and IT professionals found that three-quarters of businesses don't have a plan to respond to a cybersecurity incident. Further to this, almost half (45%) of those companies with a process in place don't test it enough to stay up to date.

These findings are even more concerning in light of research published by the Department for Digital, Culture, Media and Sport, suggesting that every data breach or cyber incident results in losses of £4,180 on average - up from £3,160 in 2018 – for businesses.

Although the study targeted relevant industry professionals, the fact is that data and cybersecurity are no longer considered just the responsibility of the IT department. All employees are accountable for maintaining data security, regardless of organization type or sector.

Thankfully, there are several internationally recognized standards that companies can use to guide their data management. Standards, such as ISO/IEC 27001 Information Security Management, help inform new processes, improve employee training procedures and ease legislative compliance; while others, like BS 31111, help managers understand the cyber risk landscape to build resilience against cyberattacks.

New standards are also being introduced to keep up with the ever-changing cybersecurity landscape. For instance, ISO/IEC 27701 Privacy Information Management – an extension to ISO/IEC 27001 – provides specific guidance on privacy protection through optimized personal information management. The standard helps companies build trust and increase transparency – clarifying key roles and responsibilities for all staff.

An important element of good data privacy is secure storage. With cloud services now the norm, it's critical to select the right provider. There are three related standards to help organizations make informed choices and then manage their storage arrangements in partnership with their selected cloud partners. ISO/IEC 27001 and ISO/IEC 27002 are used to optimize cybersecurity, while ISO/IEC 27017 aids with cloud service specific controls.

Any kind of data loss or security breach is bad for businesses – it damages trust, can incur fines and draws unwanted attention to the company. The GDPR introduced strict penalties for non-compliance, unequivocally placing responsibility with the organization, giving EU residents and citizens ultimate control over their personal information.

Key Data Management Standards

PROTECTING COMPANY INFORMATION

ISO/IEC 27001

Information technology – Security techniques – Information security management systems – Requirements

ISO/IEC 27002

Information technology – Security techniques – Code of practice for information security controls

ISO/IEC 27003

Information technology – Security techniques – Information security management system implementation guidance

ISO/IEC 27005

Information technology – Security techniques – Information security risk management

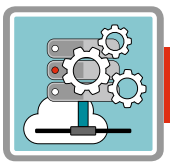
BS 7799-3

Information security management systems – Guidelines for information security risk management

PROTECTION AGAINST CYBERASSAULTS

ISO/IEC 27032

Information technology – Security techniques – Guidelines for cybersecurity



DATA MANAGEMENT AND CLOUD STORAGE

ISO/IEC 27017

Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services

ISO/IEC 27018

Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

ISO/IEC 27701

Privacy Information Management – Security techniques. Extension to ISO/IEC 27001 and ISO/IEC 27002. Requirements.

BS ISO/IEC 19944

Information technology – Cloud computing – Cloud services and devices Data flow, data categories and data use

It's also important to remember there are over 100 other different territorial data privacy regulations – each with varying requirements and stipulations. BS 10012 helps companies define their GDPR risks and compliance requirements, then implement a personal information management system in a way that's best for their business.

Employee awareness and understanding of data security and privacy responsibilities are critical to reduce organizational risk. Creating a clear policy for all staff, in line with ISO/IEC 27001 requirements, is the best way to mitigate threats to security. It's worth consulting ISO/IEC 38500, which provides guidance for IT governance. Regular, tailored training and engagement sessions keep staff focused on their collective responsibility. This is also critical to help reduce the human error factor.

Using recognized standards to inform data protection and privacy processes helps companies understand their current, and potential, levels of exposure and provides a framework of controls to manage or reduce them. Selecting and managing the right group of standards for your company is easy with BSOL, a simple online tool that gives you instant access to the standards you need. It's easy to build your own database of relevant standards, access everything you need digitally and stay right up to speed with the latest updates and revisions.

Finally, certification helps to gain stakeholder and customer trust, providing reassurances that their personal data is protected, and often providing a boost to corporate reputation in the process. It also increases transparency between supply partners, reassuring all parties that appropriate controls are in place and pushing accountability far down the chain.

The five Ws of data security

BS 10012 helps companies manage the five Ws of data, namely:

1. Whose data is it?
2. Why are we processing it?
3. Where is it kept or transferred to?
4. When are we keeping it until?
5. What safeguarding mechanisms do we have in place?

bsi. BSOL
Standards Online

The reassuringly easy way to work with standards

BSOL is a simple online tool that gives you instant access to the standards you need, making life a lot easier. It's easy to build your own database of relevant standards. Then you can find what you need fast and stay right up to date – so you can avoid costly errors and work with confidence.

Know you're covered

Save time
Manage all your standards in one place. You can access ISO, EN, BS ASTM and IEC standards through BSOL – and it takes only seconds to search.

Save money
Make standards even better value for money. Using BSOL gives you large savings on your traditional standards spend.

Miss nothing
Get an alert whenever a standard changes and understand the significance immediately. Then view the differences to key standards, so you can track exactly how they've changed.

Reduce risk
Track past, present and future changes. With access to historic and emerging standards, you can see the guidance that informed previous decisions, as well as changes that could shape your future moves.

Fit the way you work

Tailored to you
Subscribe only to the standards you need, use pre-built modules or build personal collections.

Full flexibility
You can still access every standard in the system and update your choices at any time.

Easy monitoring
Monitor which standards your users are working with, and easily spot gaps or overlaps.

Free and unlimited training
Our training team are here to give you extra support if you need it.

Make life easier with BSOL.

Get a quote or find out more at bsigroup.com/bsol.
Or call +44 (0)345 086 9001.

bsi.

...making excellence a habit.™

MANAGING DATA WITH CONFIDENCE

Key Data Management Standards

ISO/IEC 27701

Privacy Information Management – Security techniques.
Extension to ISO/IEC 27001 and ISO/IEC 27002. Requirements.

BS ISO/IEC 19944

Information technology – Cloud computing – Cloud services and devices data flow, data categories and data use.

ISO/IEC 27032

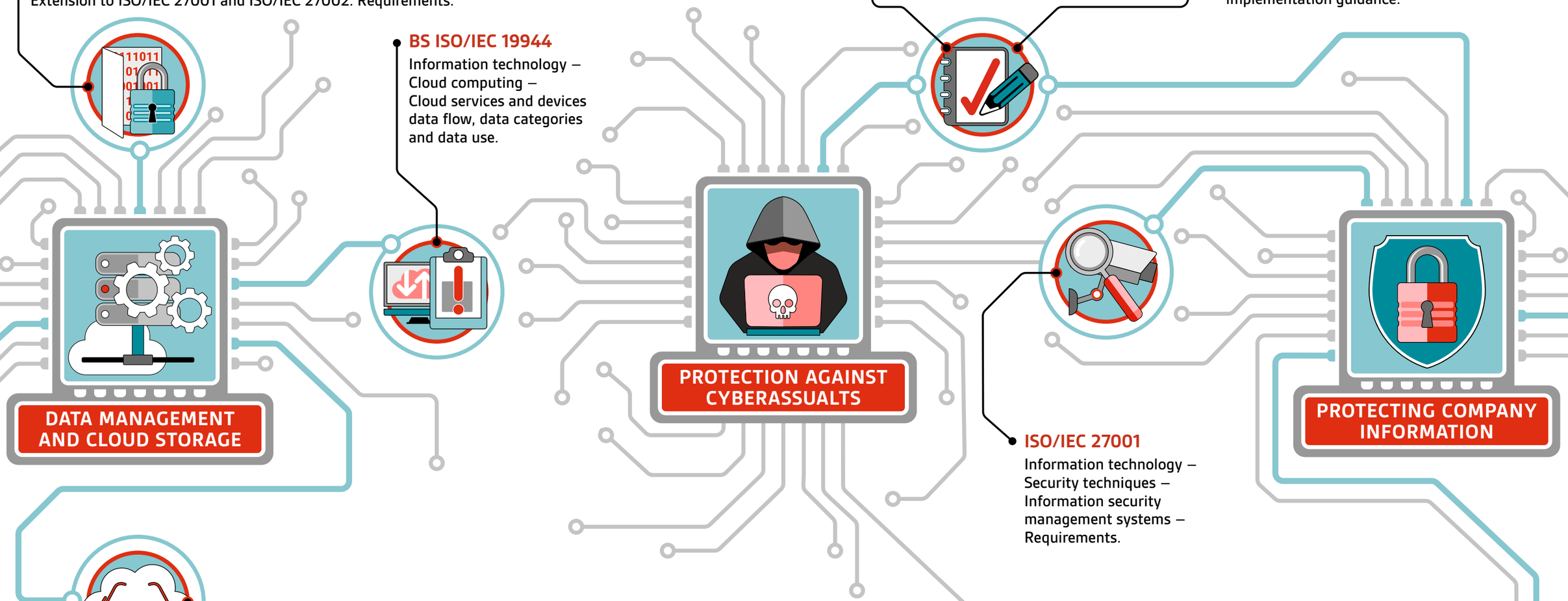
Information technology – Security techniques – Guidelines for cybersecurity.

ISO/IEC 27002

Information technology – Security techniques – Code of practice for information security controls.

ISO/IEC 27003

Information technology – Security techniques – Information security management system implementation guidance.



ISO/IEC 27001

Information technology – Security techniques – Information security management systems – Requirements.

ISO/IEC 27017

Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services.

ISO/IEC 27018

Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.

ISO/IEC 27005

Information technology – Security techniques – Information security risk management.

BS 7799-3

Information security management systems. Guidelines for information security risk management.