BYTES | Smarter together

Bytes Cyber Consulting

Take swift action where it counts, protecting your business and your customers from genuine risks in the most effective way.

Contents

About Bytes
Cyber Consulting

How should you prioritise your security today — when the threat landscape is shifting constantly and the compliance environment is getting tougher? After all, resources are limited and it's impossible to secure everything to best practice.

With Bytes Cyber Consulting, you can act where it counts, protecting your business and your customers from genuine risks in the most effective way. We'll help you to spot security threats, vulnerabilities and weaknesses, whilst finding practical answers and solutions that may lead to greater opportunities in cost reduction or revenue generation.

We don't just advise, **we deliver**

Three reasons why businesses **trust us on security:**

1. Experience
We understand security inside out, across your business. We have more than 20 years of experience working with leading enterprises and countless user environments, across all sectors.

2. Insight
We know where gaps exist and how to fix them. Our consultants have worked for or in key vendors, service providers, value added resellers, system integrators, major consulting houses and law enforcement – so we have it covered.

3. Action
Based on our experience we know that what you need is a solution to the problem. So, we don't just conduct audits, assurance testing and expert analysis. We provide practical and flexible real-world solutions, virtual services and support, to help keep you secure.

Let's get to work on your objectives

We're easy to partner with, we engage at a fair price and we provide business-aligned results — by following a proven consultative approach.

Our services are delivered by senior level and experienced consultants with the right certifications. Having defined and agreed what's needed, we'll keep your projects on track and on budget.

Our expert consultants are perfectly placed to guide you through the smoke and noise of the security arena.

Let's find answers quickly to your most pressing issues today — and act wisely to create a secure tomorrow.

We understand the challenges you're facing

Cyber security is becoming increasingly complex for organisations of all sizes, the world over. Today, there's a far greater likelihood of security controls failing, leading to information leakages and breaches. We believe this happens because of a series of factors:

| Attackers | + | Punitive regulation | + | Material fines | + | Technical / business complexity | + | Rapid adoption of change | = | Instability |

Instability is what causes security incidents. This coupled with the complexity of frameworks, competing and conflicting requirements as well as ever increasing speed of change in technology makes securing companies even more challenging. It is our belief that this is only going to get more troublesome and onerous over time. As such, you need a simple solution that will help in one, or multiple aspects of security. See how we can help, not just today, but tomorrow and into the future.
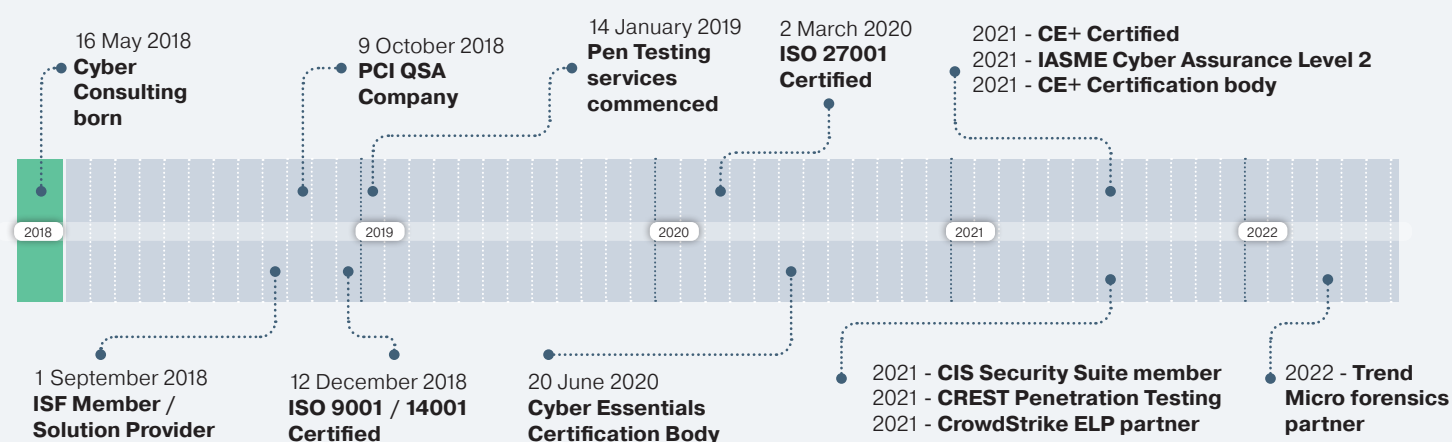
Together, we'll find simple answers to complex challenges

Bytes Cyber Consulting helps companies to adapt to new threats and realities in an effective way, so they spend wisely and focus more of their resources on key business goals.

As a division of Bytes, we provide best-in-class security consulting, security strategy, assurance testing, as well as digital forensics and incident management services.

We've built a strong reputation, working with a multitude of clients and leading security vendors, using our deep experience to find the simplest answers to serious problems. Our approach works, whether we're tackling a single issue or helping our clients to sharpen their entire strategy.

Cyber Consulting Timeline

16 May 2018
Cyber Consulting born

9 October 2018
PCI QSA Company

14 January 2019
Pen Testing services commenced

2 March 2020
ISO 27001 Certified

2021 - **CE+ Certified**
2021 - **IASME Cyber Assurance Level 2**
2021 - **CE+ Certification body**

2018   2019   2020   2021   2022

1 September 2018
ISF Member / Solution Provider

12 December 2018
ISO 9001 / 14001 Certified

20 June 2020
Cyber Essentials Certification Body

2021 - **CIS Security Suite member**
2021 - **CREST Penetration Testing**
2021 - **CrowdStrike ELP partner**

2022 - Trend Micro forensics partner

How we'll help your team to succeed

Our portfolio of cyber security services is comprehensive, combining security, technical know-how and qualifications with information and cyber security good practice underpinning corporate credibility.

Audit & Advisory	Strategy	Assurance
Payments & PCI DSS	ISF Security Healthcheck & Benchmarking	Penetration Testing
Data privacy services		
ISO 27001 advisory services	Cyber strategy & cyber resilience	
Cyber / information / technology security frameworks	vCISO service	Digital Forensics & Incident Management
Cyber Essentials		
Digital footprint, risk & threat assessment	Project & 3rd party security reviews	

If you don't see the service you want, get in touch and we'll be glad to help.

Company credentials

iSF Member

CYBER ESSENTIALS CERTIFIED

QMS ISO 27001 : 2013 REGISTERED

ACS REGISTRARS Quality Assurance ISO 9001

ACS REGISTRARS Environmental Assurance ISO 14001

Chartered Institute of Information Security

Consulting credentials

CREST   PEN TEST   PCI QUALIFIED SECURITY ASSESSOR   CYBER ESSENTIALS PLUS   iSF Solution Provider   POWERED BY CROWDSTRIKE ELP Forensics Partner   digital shadows

TRUSTED PARTNER 2021 - 2022   Chartered Institute of Information Security   iSF Member   CIS SecureSuite Membership

Cyber resilience and cyber strategy

This is the perfect place to begin. Resilience is the capacity of an ecosystem to adapt to change and disturbance by resisting damage and recovering quickly. With Bytes, you can strengthen your resilience at a core level — and maintain your capabilities over time.

We know the landscape

As companies evolve, they often fail to keep up with cyber security. But our experienced consultants will help you to fix that. We offer flexibility — so you can pick the services that you want and do as much or as little in-house as you wish. Our services are designed to be complementary and can be built up over time.

Cyber resilience

Maintain / certify

Implement   **Test**

Review and strategy   **Risk control planning**

Internal healthcheck   **Third party healthcheck**   **Vulnerability and threats**

The number of frameworks and controls can seem mind-boggling and in conflict at times. The key is to focus on risk management and the application of aligned control sets. We'll help you to do this

Let us turn complex into simple

The ISF Standard of Good Practice (SoGP) can sound daunting, with its 4000-plus controls. Some companies get lost in the complexity. However, we'll show you how frameworks can be used effectively and fit together to increase coverage and depth of protection.

Staying mission-focused

We start with identifying your needs and desired outcomes, before evaluating the maturity of your organisational and technical controls. We can then pinpoint exactly where you need to prioritise.

All security requirements (ISF SoGP)						
Information Security Management / Assets (ISO 27001)			Governance (Cobit 5)	Third Parties (ISO 27001)	IT (Cobit 5)	Risk (ISO 3100 / IRAM2)
Privacy assets (DPA / GDPR) (ISO 27701)	Commercial general requirements (ISO 27001)	Government general assets (ISO 27001)	Information security governance (ISO 27014)	Suppliers (ISO 27036)	Asset control (ITIL / ITSM)	Information risk management (ISO 27005)
Payment assets (PCI DSS)	Commercial specific assets (Per contract requirement)	Government specific assets (Co Co / RMADS etc.)	Specific governance (NCSC / other recommendations)	Supplier specific requirements (As per contract)	Technical security (ISO 27002, NIST, CIS, SANS, GPG's etc.)	Specific risk management (As required - COSHH, OHAS etc.)

Our expertise extends across key frameworks. These can be tiered to provide aligned control sets.

With Bytes, you can mix and match a range of services …

Check your defences
- Get an ISF security healthcheck
- Assess your supply chain
- Test your exploitability

Sharpen security
- Get leading security expertise
- Select the right solutions and re-run tests
- Evaluate certification readiness

Think strategically
- Review findings with your board
- Plan the best strategic response
- Align plans with your business

Maintain & certify
- Implement KPIs to measure controls
- Formalise processes at highest level
- Work towards certification

Let's work in stages, aligned to your business requirements

Achieving your goals doesn't have to be cumbersome. The key is to adopt an approach based on business need and maturity — taking the right step at the right time.

We can help you decide the best approach. Here are examples of four areas you may wish to prioritise, depending on your scenario:

People
- Help with identification of assets
- Take ownership for protection
- Follow and apply protection processes

Process
- Alignment of security with business process
- Automation and repeatability
- Threat and risk assessment
- Communication

Information
- Identification of the 'crown jewels'
- Tiered security based on risk and value of the information
- Information classification, handling, labelling and watermarking

Technology
- Robust IT and technical security standards
- Basic security controls (hardening, patching, AV etc.)
- Advanced security controls including IAM, DRM, DLP, IPS, WAF, memory analysis etc.
- Monitoring & alerting

ISF Security Healthcheck & Benchmark

Do you ever wonder how secure you really are — and how you measure up against your peers? It's an issue that's commonly raised in the boardroom, especially relating to focus and expenditure. Bytes can provide the deep insights you need.

Getting the clearest picture

Every team needs to have a sense of how their Cyber or Information Security approach is performing against what's normal in their industry. Traditionally, this has always been hard to answer because reviewing against one standard often gives a one-dimensional and incomplete picture.

At Bytes, we do things differently. We use the ISF Security Healthcheck and benchmark, which is the most comprehensive assessment available globally, allowing us to deliver quick and meaningful answers.

One assessment, multiple outputs

Gone are the days when you need to do more than one assessment. Our consultants can assess you against the ISF Standard of Good Practice and our automated tool does the rest ... with one assessment we can tell you your cyber maturity against these standards:

· Information Security Forum (ISF) Standard of Good Practice (SoGP)
· ISO 27002 and NIST Cyber Security Framework
· CIS Top 18, COBIT 5 and PCI DSS

How do you stack up against your peers?

Knowing how you compare against your peers is important, so you can justify your approach and budgets. We make your results anonymous and measure them against your industry sector in any region or globally, using ISF data from other participating companies and consulting assessments. We'll optimise the output against any standards, as maturity levels vary greatly per region.

What does maturity mean anyway?

Maturity is critical to success. The more mature your controls, the more complete the coverage and the more protection you have. It's important to see which controls are working at optimum levels for your business and risk profile — and identify those that need more attention. Our consultants will provide the answers so you can increase your maturity over time.
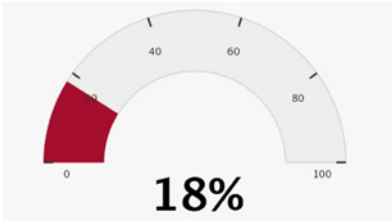
What does the healthcheck and benchmark show me?

With Bytes, there's no guesswork — or ploughing through hefty tables and endless reports. You can get straightforward answers that'll carry weight in the boardroom.
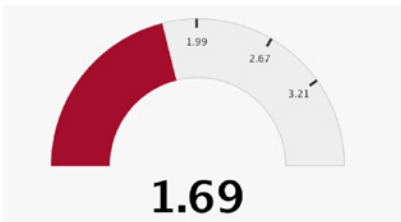

How do you compare?
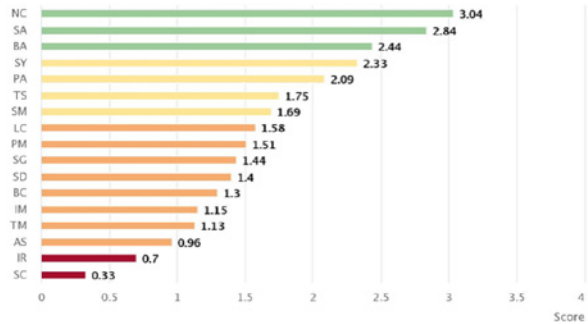Discover how your controls stack up against your peers.

Percentage of peers exceeded
Find out how many peers you exceed for the security controls you apply. Compare by geographical region, industry vertical or both.
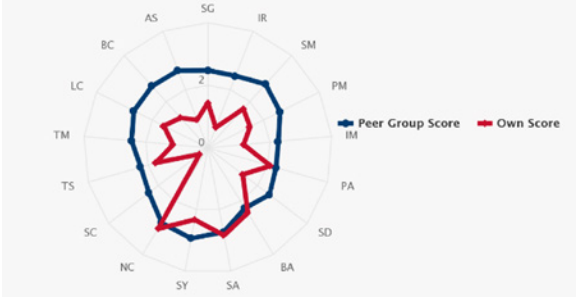
Quartile breakdown
Discover how much you need to improve overall to raise your maturity level — to a level that meets your risk appetite.

Ranking scores
Bytes will rank your areas of strength and those that need improvement. See the variance of controls across your business and how much effort will be required to improve. Our consultants can help you to maximise your performance.

Peer group comparison
See how you compare to your peer group and your own previous assessment. Identify the areas where you do well and need to continue and those where more resources are required to improve.

	SH	SH+	SH++
Self-assessment questionnaire	✔	✔	✔
Benchmark against your peers	✔	✔	✔
Automated reporting	✔	✔	✔
Focused strategic consulting report to improve		✔	✔
Containment audit		✔	✔
Full external audit			✔
Single standard feedback on scoring			✔
Single standard improvement plan			✔

Choosing the option that's right for you

Why not benchmark other companies that impact your business?

Our clients use this automated service to assess third parties to see how they stack up against their own industry standards. Some of our clients also use this service for mergers and acquisitions, gaining valuable insights at pivotal moments.

Assurance - Penetration Testing

It's important to be able to reduce the risk of security incidents dramatically. That process begins with understanding vulnerability. Our team has the tools and expertise to help.

We offer three simple approaches. Choose the one that best fits your needs…

Where are you at risk?

How secure is your core infrastructure, your mobile apps or your cloud deployments? How well can you protect yourself against a physical breach, social engineering or inside threats? Bytes can provide an accurate picture - so you'll know exactly what action to take today.

Minimising vulnerability

Penetration testing and assurance services from Bytes will enable you to minimise the window of opportunity for attacks, guard against systemic failings and identify simple errors that widen your vulnerability. With our help, you could reduce security incidents by up to 95%.

Finding backdoors

We offer a blended approach to testing - from the essentials of a vulnerability assessment, right up to the scenario of a rogue employee joining your team and working as a system admin. Our experts will find the backdoors you didn't know existed and help you to close them. We'll also enable you to build up wider intelligence about how your environment and people operate.

Keeping it real

The last thing you need are theoretical exploits or false positives. Our testers use the tools and automated techniques common across the industry, but we only focus on genuine areas of risk in our reports.

Offering flexibility

Our service can adapt to suit your objectives. Use our testers when you want them. We'll work to your budget and have the results in a format you can use. Our team will support you through the process.

Sharing expertise

We take a collaborative approach and will transfer knowledge to your team about the security testing process. As a result, you'll be able to avoid many common mistakes in the future, boosting your security.

Where do you want to start first?

We'll work with you to identify your priorities. Our services can include:

- Infrastructure testing, including vulnerability analysis, VLAN and containment breakout
- Build reviews, covering firewall/router rule sets, systems, mobile devices and more
- Cloud testing, including Azure and AWS testing, plus IaaS, PaaS, public, private and hybrid
- Application testing, from web and mobile to client-side applications and API manipulation
- Covert testing, including social engineering and insider threats with/without privileges

You can trust our expertise.

We are a CREST Penetration Testing Company, and our expert team includes CREST certified testers.

---

1. Snapshot:
A great place to start

Ideal for smaller organisations and those starting out with security testing, the Snapshot is like an MOT that covers the basics. You can then make risk-based decisions about your points of exposure - and we'll tell you how to fix them.

2. Optimise:
Get straight to the fix

Why pay for formalised, regulated tests - when you can get right to the heart of your security at any time? Our experts will identify the key risks, the issues and how to fix them. We'll put the facts at your fingertips.

3. Complete:
When you need to go deep

We have a test for virtually everything - and we can even provide someone to work covertly within your operation. Get full reporting and access to our test base throughout the testing phase and while you carry out remediation.

Services / Features	Snapshot	Optimise	Complete
Vulnerability analysis	✔	✔	✔
External infrastructure	✔	✔	✔
Firewall / router rule set reviews	✔	✔	✔
Insider threat with and/or without privilege	✔	✔	✔
Internal infrastructure		✔	✔
VLAN / containment breakout		✔	✔
WIFI		✔	✔
Secure services break out (Citrix, terminal services, VDI)		✔	✔
Azure and AWS security testing and remediation solutions		✔	✔
Systems and mobile devices			✔
Static and dynamic code review			✔
Technical remediation and security hardening techniques			✔
IaaS, PaaS, public, private and hybrid cloud			✔
CDN breakout and origin exposure exploitation			✔
Web applications			✔
Mobile applications			✔
Client-side application testing			✔
API manipulation and testing			✔
Reconnaissance and intelligence gathering			✔
Social engineering			✔
Physical breach			✔
PCI DSS - covers requirements: 1.2.1, 1.2.2, 1.2.3, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.6, 1.3.7, 2.1, 2.1.1, 2.2.1, 2.2.2, 2.2.3, 2.2.4, 2.2.5, 2.3, 4.1, 4.1.1, 5.1.2, 6.2, 6.6, 11.1, 11.3, 11.3.1, 11.3.2, 11.3.3			✔
ISO 27001 - covers requirements: A12.6.1, A13.1.1, A13.1.2, A13.1.3, A14.1.2, A14.2.3, A14.2.8, A14.2.9, A18.2.3			✔
Any other form of testing			✔

Want to change testing companies regularly?

Not an issue, use Bytes brokerage service to manage all testing in one place, same contract and pricing, using one of our approved CREST / CHECK certified partners.

Compromise Assessment

Ideally, organisations should combine penetration testing with a Compromise Assessment for a well-rounded approach to technical security.

A penetration test can only tell you what your vulnerabilities are — not whether these have been exploited. A Compromise Assessment will tell you if these have been exploited and whether you should be concerned about a security incident or a data breach event.

Understanding the landscape

It's estimated that over 50% of breaches are missed by existing cyber defence tools. This is a frightening statistic and is probably caused by increases in the sophistication of the tools that threat actors use. Most current sophisticated threats use file-less injections that live in memory and these are very hard to prevent, let alone detect.

What is the risk?

The current threat landscape has seen a marked change in attack sophistication and the way that companies are compromised. Now, simple rules-based, or Macro-based attacks, are used to target end users on a widespread basis. Once an attacker has you on the hook, they then assess you. Once your company has been classified, access is sold to a third party that's motivated to attack.

They will use the entry point to move laterally, seeking what's valuable and living off the land to avoid detection. This will then result in strategic data removal, targeting of financial assets, or ransomware events to extort money.

What's your best response?

A Bytes Compromise Assessment uses a state-of-the-art endpoint detection and response platform — so our forensic consultants can quickly hunt, detect and respond to advanced cyber threats, risks and vulnerabilities at scale inside your organisation. The solution complements your existing endpoint products (AV, EDR, SIEM and SOAR products). It also allows us to test and validate your security controls and compliance, while providing detailed post-incident assessments that verify and validate your overall security posture.

How do we do it?

Our forensics consultants will work with your internal IT or security teams to deploy a central collection server (for agentless scanning) or real-time protection agents to each host. We follow a simple but aligned, forensically-sound methodology to achieve this ...

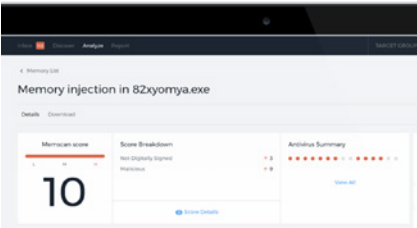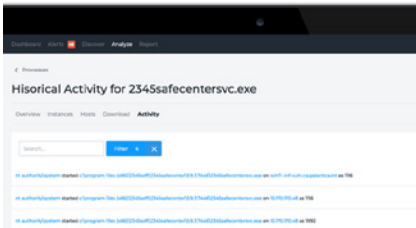| Setup & installation | Initial deployment & scan | Data scanning analysis | Threat assessment | Containment | Eradication | Re-scan until clean |

Every step is carried out remotely. We can offer this solution anywhere in the world and start detection in minutes, not hours. We operate at speed and scale, no matter how large the network. Our forensic consultants can work proactively or reactively, providing the expertise to interpret the results, remove false positives and assist with any remediation.
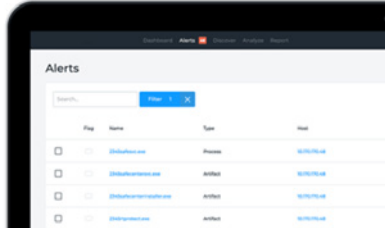
File-less threat detection and response

Modern attacks and malware target memory. Antivirus software and endpoint security tools are limited in their ability to detect file-less threats. We inspect the memory across your endpoints, closing the detection gap for stealth attack techniques.
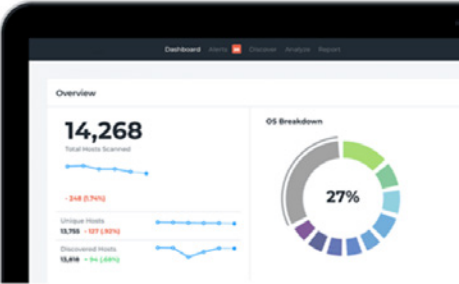
Advanced forensic analysis

We can combine historical forensic data with real-time event data so you can quickly determine root cause, identify patient zero and investigate unknown cyber threats.
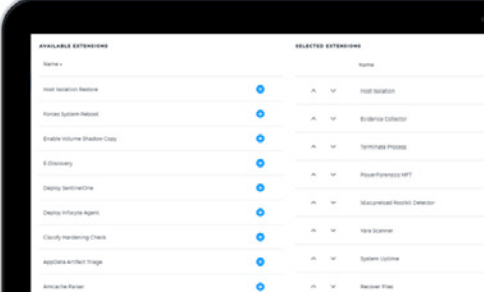
Real-time data

Bytes will hunt in real-time for advanced cyber threats across your environment. This includes Apple, Windows, Linux and Unix devices that may be on-premises, in a datacentre, in the cloud or part of a remote workforce.

Agentless assessment

For centralised systems Bytes can scan using agentless techniques. We can get scans up and running in minutes and produce results quickly.

Automated remediation

Bytes can use the solution to isolate affected systems and then conduct automated remediation. This can be completed globally against all assets in the platform at scale, to restore normal service quickly.

A valuable service for mergers and acquisitions

Thinking of buying another business? Do you know what you are buying and your risks of regulatory, legislative, or contractual losses? Bytes customers use this service to evaluate the companies they are buying. You can then make better-informed decisions on the purchase price!

Cyber Essentials

Why Cyber Essentials?

"Cyber Essentials is a simple but effective, Government backed scheme that will help you to protect your organisation, whatever its size, against a whole range of the most common cyber attacks.

Cyber attacks come in many shapes and sizes, but the vast majority are very basic in nature, carried out by relatively unskilled individuals. They're the digital equivalent of a thief trying your front door to see if it's unlocked. Our advice is designed to prevent these attacks."

The NCSC

Whether you're looking to improve your basic security, or be part of the government supply chain, Cyber Essentials is a scheme worth considering. It's available from Bytes.

The 5 technical controls for Cyber Essentials:

1. Secure your internet connection	**2.** Secure your devices and software	**3.** Control access to your data and services	**4.** Protect against viruses and other malware	**5.** Keep your devices and software up to date

Get the most from Cyber Essentials

Cyber Essentials really does help you get the basics of Cyber Security right. You cannot FAIL any of the controls, but you are allowed 2 MAJORs and the Bytes team can guide you through the process.

We have our own in-house teams to conduct Cyber Essentials. But we also use the best on the market, acting as a broker on your behalf. That way you can be assured of the best price and quick availability.

We offer three levels of services:

Certification	**Optimise**	**Complete**
Certification audit only	Pre-assessment review of information and feedback on compliance status followed by certification audit	Full lifecycle of gap assessment and remediation action plan, pre-assessment and certification audit

Choose your level of service and the certification standard you require:

	Cyber Essentials	Cyber Essentials Plus
IASME Cyber Essentials certification	✔	✔
IASME Cyber Essentials Plus certification		✔
Cyber liability insurance*	✔	✔
IASME certified consultant	✔	✔
Free re-submission within two working days	✔	✔
External infrastructure vulnerability assessment		✔
Remote or on-site** technical audit of in-scope systems including user devices, internet gateways and services accessible to unauthenticated internet users. Sample size can be up to 10%***		✔
Same day start or to your schedule	✔	✔

* see https://iasme.co.uk/cyber-essentials/cyber-liability-insurance/ for more details on the included cyber liability insurance, and if you qualify
** subject to expenses
*** The technical test specification from the NCSC can be found here: https://www.ncsc.gov.uk/files/Cyber-Essentials-Plus-Illustrative-Test-Specification-April-2020.pdf

Payments & PCI DSS Audit & Advisory Services

Any forward-thinking merchant or service provider understands the value of being able to accept secure payments across multiple channels. If you're not at the leading edge, you could miss out on extra business as well as getting targeted by fraudsters.

But Bytes can help.

The payment world is changing

The UK is moving swiftly towards being a cashless society: Cards, mobile transactions and new payment methods are growing in popularity. Meanwhile, out-of-region payment solutions and services - from China Union Pay to dynamic currency conversion - are becoming ubiquitous with consumer expectation for acceptance. But these solutions cause not only acceptance issues for merchants but new fraud attack surfaces. In addition, GDPR and the Data Protection Act 2018 have raised the stakes. Suffer a breach and the likely fall-out and fines have never been more expensive or damaging to company reputations.

PCI DSS with a difference

At Bytes, we recognise the importance of the Payment Card Industry Data Security Standard (PCI DSS). But we don't merely help you to jump through the hoops every year - just to gain compliance. We understand the bigger picture: Secure payments must come first and then PCI DSS compliance is gained as a by-product of good practices. We'll help you to stay secure, so you can boost your bottom line.

Trust our expertise

Our consultants have deep experience in the secure payments arena, working with many leading organisations. Our team has over 13 years as QSAs and many have also been core PFIs, so you can use their experience to avoid common mistakes and seize fresh opportunities. Whether you are a merchant or a service provider, we'll help you to maximise revenues, prevent breaches and minimise audit costs. We're skilled in scope reduction, data discovery, solution design and testing.

The Bytes approach to secure payments gives you the edge

Grow revenues
Let customers use their preferred payment methods, discounts and loyalty programmes across all your channels. Benefit from automated reconciliation to reduce team frustration and increase productivity.

Stay compliant
Protect data as close to the inception point as possible. We'll help you to leverage compliant third parties - and use artificial identifiers to keep data safe.

Self-fund security
Increase working capital and reduce the weighted average cost of credit (WACC) – which could help to self-fund the payment solutions you use.

Data Privacy Services

Confusion exists around data protection. But the goal is simple: Open, honest and transparent processing of personal data, while being accountable for the security and usage of the personal data in your care. With Bytes, you can prioritise what really counts and get peace of mind.

Cost-effective data protection

Our team will look at your data handling processes, we'll spot any gaps and issues and then carry out remediation. This allows you to be more focused and spend money more wisely within your organisation to protect both internal data as well as information belonging to customers.

We can provide a raft of expert services that meet data privacy requirements and raise the general security of your environment. These can range from data discovery and assurance testing, through to incident response services, training and the provision of a virtual Data Protection Officer.

Taking a standards-based approach

Much has been written about the GDPR, Article 42 and the certification methods that will be used to demonstrate compliance (specifically relating to Article 25(3), 32(3) and to support Article 46(2)f). Updated guidance suggests that the latest ISO standard, ISO 27701, may support the provision of GDPR certification.

Our consultants work with the ISO 27000 series of standards and are well placed to help you as an organisation ensure you can meet the requirements. In combination with ISO 27001 for information security management, uplift and alignment to support privacy information management is a simple extension.

You can focus on the areas that matter and what the ICO has identified as important

Awareness	Information you hold	Communication	Individual rights
Subject access requests	Legal basis for processing	Consent	Children
Data breach	Protection by design	Data Protection Officer	International

Working through the standards, article-by-article can be difficult and cumbersome. Let our consultants work in unison with your business processes and objectives, to weave data protection and security in transparently to your services.

Overcome uncertainty
Get leading expertise on all aspects of data protection — from professionals that understand the nuances and risks.

Cover the essentials
Take advantage of our leading data privacy strategies, data discovery services, assessments and technical control solutions.

Get expertise on demand
There's no need to hire your own in-house specialist. Our virtual Data Protection Officer service can provide round-the-clock support.

ISO 27001 Advisory Services

Achieving and maintaining ISO 27001 doesn't have to be complex and costly for your business. Our professionals can help you from the start in gaining management support and then provide expertise at any stage, right up to the point of pre-certification audits.

Hitting the right standard
ISO 27001 has become the mainstay of information security standards with its usage increasing. The UK has the second highest number of certifications worldwide, following Japan – where it is a mandatory requirement for security when processing privacy data.
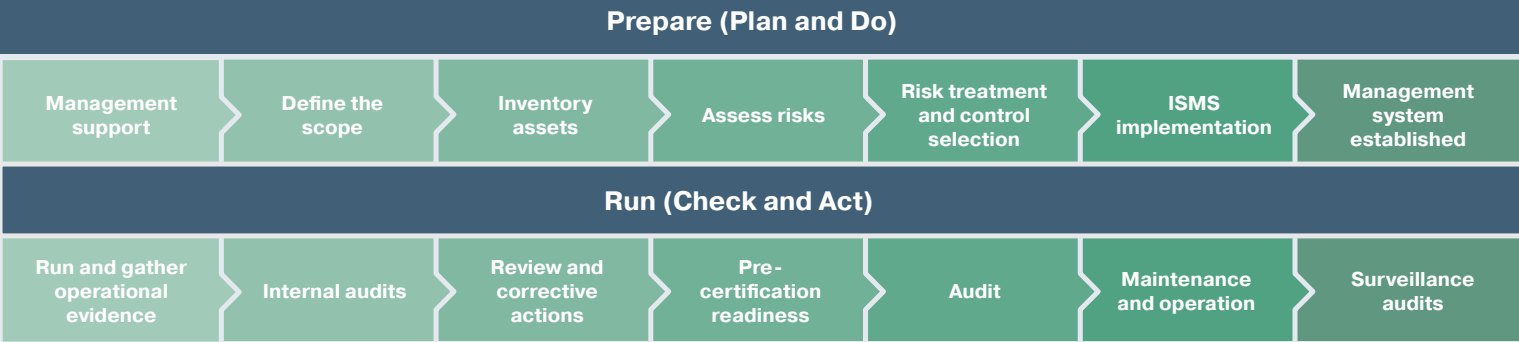
Expert help available
Bytes can help you through the process. We have consultants that hold both (Senior) Lead Implementer and Lead Auditor qualifications and have been through the process of achieving ISO 27001. We know what it takes - and the most cost-effective route for your organisation.

Keep on top of quality
Our ISO 27001 services enable you to focus on what is important to optimise both your protection and spend, using a structured framework. That means no more gaps, no more spend on unnecessary solutions - just simply use our services to keep up with your business needs.

Our methodology is simple:

Prepare (Plan and Do)

Management support	Define the scope	Inventory assets	Assess risks	Risk treatment and control selection	ISMS implementation	Management system established

Run (Check and Act)

Run and gather operational evidence	Internal audits	Review and corrective actions	Pre-certification readiness	Audit	Maintenance and operation	Surveillance audits

With Bytes, you can benefit from our expert support in key areas …

Setting the right course
✔ Management support with building your business case
✔ Defining the scope of what you need to cover
✔ Creating your inventory of information assets
✔ Conducting a risk assessment that's business focused
✔ Selecting the right stance around risk and control

Getting to your goal
✔ Creating an ISMS implementation programme
✔ Establishing a management system for policies and controls
✔ Gathering operational evidence from operating the ISMS
✔ Internally auditing the ISMS controls to check effectiveness
✔ Reviewing results and carrying out corrective action
✔ Preparing your team for the certification audit

Virtual/Outsourced CISO Service

Assurance - Digital Forensics & Incident Management

Our **Incident Response** number is: **0203 327 0698**

Today's threats have become more diverse and sophisticated, often making the security environment more complex, restrictive and costly to manage. But it doesn't have to be this way. Bytes provides enterprise-grade strategic expertise when it's needed.

Preparing for an incident before it happens, or responding to one afterwards, requires a team you can trust. With Bytes, you can have complete confidence. Our approach is game-changing.

Slipping between the gaps

Requirements for information security usually fall somewhere between technical security and legal departments — but sometimes these teams fail to grasp the bigger picture of business need and direction. They don't see how the business uses and controls its data, both inside and outside of the organisation. Without a strategic approach, companies can end up adopting a 'control by contract' attitude, spending a fortune on equipment and placing heavy restrictions on business operations and how staff work.

C-suite level insights

Bytes can provide the expertise, flexibility and forward-thinking you need with our virtual/outsourced CISO service. This service is led by Bytes' own CISO, so we can give you the kind of strategic guidance that a Chief Information Security Officer at a world-leading enterprise would offer. You can get a cohesive and cost-effective plan that works.

We're a mission-critical part of your team

Our virtual CISO acts as an extension to your business and adds value to your organisation with a proven methodology, based on years of experience working with leading enterprises. We'll help you to set the strategy, we'll work closely with your board, help you to establish an internal delivery team and provide ways to monitor day-to-day performance, while keeping you in total control.

Our approach uses the best from NIST 800-61 and the CREST CSIR methodologies by following the same process for security incidents:

Preparation	Identification (detect & analyse	Containment	Eradication	Recovery	Lessons learned

In one sense, there's nothing new here. As you would expect, we use seasoned professionals, with the unit being run by ex-police personnel. But the real game-changer is our responsiveness.

The new world of digital forensics and incident management

Bytes has revolutionised its response services to meet the modern era. We combine senior resources remotely, with the ability to reach into a network and conduct a full incident response process. This way you do not have to wait for people to arrive. Bytes has a state-of-the-art cloud-based forensics lab that can respond to incidents anywhere globally. Our threat hunting and forensic analysis platform allows us to reach in quickly, while following forensic methodology.

Our process follows a tried and tested methodology

Review business strategy	Establish security baseline	Establish risk appetite	Board review and steering	Business aligned security strategy	Implementation oversight	Maintenance and certification	Management security forum

How do we do this?

Preparation starts with a few clicks. We can perform secure, targeted collection of digital forensic evidence simultaneously across your endpoints.

It takes minutes not hours to acquire information, start the identification process and begin to detect and analyse the issues.

Containment of the endpoint(s) occurs by silently blocking malicious activity or locking down endpoints entirely, so eradication can begin.

Recovery can be conducted via automated remediation against all assets in the platform, to restore normal service quickly, while preserving evidence.

We can forensically report and then debrief the teams on the findings, so that any lessons learned can be actioned quickly.

With Bytes, you can get security that fits your business precisely…

Covering the essentials

Set the strategy and the vision for security in a way that reflects your reputation, corporate governance and regulation, corporate social responsibility and information assurance.

Seeing the big picture

The CISO service is independent of technology or IT departments, so our experts are free to consider the environment and unique challenges of your business operation.

Acting strategically

Our professionals will understand clearly what your business requires. We'll only suggest good practice so it will add genuine value - rather than pile on unnecessary cost.

What makes us so different?

Cradle-to-grave management
- Full ownership of the incident management and forensics processes
- Management and evidence in line with court and expert witness requirements

On and off cover response
- IR retainer and preferential response
- Off cover assistance and deployment
- 24x7x365 coverage and boots on the ground in 24 hours if needed

Proactive services
- Proactive incident management services
- CSIR maturity assessments & policy updates
- Tabletop and blue team exercises
- Purple team support and evaluation

Expertise on demand
- You can talk to an expert as an extension to your own team
- Talk through problems and concerns, or have us check what your team has done

Discover more. Get in touch today,
our expert team stand ready to help.

Get in touch on:

+44 1372 418500

or **Tellmemore@bytes.co.uk**

Alternatively find us at **www.bytes.co.uk/security/cyber-consulting-services**

BYTES | Smarter
together