

Norm's Compliance Services

Norm's Compliance Services ensure that your business is doing the basics; putting in place policies, procedures and measures to protect the confidentiality, integrity and availability of your confidential information assets.

It may be dull, but process makes any organisation tick along efficiently. It's also a necessary evil if you want to achieve industry-recognised accreditations and demonstrate to your shareholders, customers and trading partners that their data is in safe hands.

Norm's Incident Response Service comprises of four key security modules:

- Cyber Essentials
 - Self-Assessment
 - Guided
 - Supported
- Cyber Essentials / IASME Governance
 - Self-Assessment
 - Guided
 - Supported
- Cyber Essentials Plus
- IASME Governance Audited / IASME Gold
- ISO27001 GAP Analysis

This service module focuses on the **Process** element of Norm's holistic trinity of cybersecurity - **People, Process and Technology**.

Its purpose is simple;

To ensure that your business has the appropriate level of information security policies and processes in place to guard against the most common cyber threats and demonstrate your organisation's commitment to cyber security.

It provides;

- * Access to our Consultants who will guide you through the compliance standards
- * Audits by our qualified assessors to examine the same controls and test that they work through a technical audit
- * Final certifications and reports with analysis and recommendations where required

A reassuringly dull description*



Cyber Essentials

Cyber Essentials is an independently verified self-assessment certification. The Certification gives you, suppliers and customers peace of mind that your defences will protect against the vast majority of common cyber-attacks simply because these attacks are looking for targets which do not have the Cyber Essentials technical controls in place.

Cyber Essentials can be obtained via three service variants:

- Self-Assessment
- Guided
- Supported

Cyber Essentials Self-Assessment Service

Provides you with access to the 'Pervade' online Cyber Essentials Accreditation Scheme Portal. There will be a series of questions that you need to answer that evaluate your basic cyber and information security controls. The five areas that will be assessed are:

- * Organisation
- * Secure Business Operations
- * Access Control
- * User Accounts
- * Malware and Technical Intrusion

Cyber Essentials Guided Service

The "Guided" service gives the same access to the 'Pervade' portal as the Self-Assessment service but also provides you with access to one of our compliance consultants who will provide up to 2 hours of remote support.

Cyber Essentials Supported Service

The "Supported" service gives the same access to the 'Pervade' portal as the Self-Assessment service but also provides you with access to one of our compliance consultants for one-day of consultancy. This can be either attended at your office or remotely delivered.

A reassuringly dull description*



How does it work?

Once your order is received, a member of our customer experience team will take ownership of your order and contact you to introduce themselves as your project lead. They will arrange a Welcome call with you to guide you through the process, outlining who will be responsible for each element of the assessment. We will then:

- Provide access to the Pervade Portal.
- Arrange for the consultancy services (for Guided or Supported service variants).
- Agree a date with you for your assessment.

You will have 6 months to complete your assessment before your account is archived. Upon completion of your Cyber Essentials question set, one of our auditors will mark your answers to check that the measures you have advised are appropriate. If your application is successful, you will be issued with your certificate.

If you fail to meet the required standard, you are allowed two working days to examine the feedback from the assessor and change any simple issues with your network and policies. You can then update your answers and the assessor will reassess your submission without further charges. However, if you still fail after these two working days you will be required to reapply and pay the assessment fee again.

Once you successfully achieve your Cyber Essentials accreditation, this enables you to display your certificate and the Cyber Essentials logos on your website/marketing material etc.

Service Availability

The Norm Compliance consultants and Customer Experience teams are available during UK business hours, Monday to Friday 9:00 to 17:30, excluding public holidays.

The Customer Experience team will be on hand to provide technical advice and assistance for any queries or issues should this be required.

Cyber Essentials / IASME Governance

IASME Governance certification is aligned to the Government's Ten Steps to Cyber Security and includes the Cyber Essentials certification in addition to controls relating to people and processes. It also covers the General Data Protection Regulation (GDPR) requirements. IASME Governance is aligned to a similar set of controls to ISO 27001 but is more affordable and achievable for small and medium-sized organisations to implement.

Cyber Essentials / IASME Governance certification can be obtained via three service variants:

- Self-Assessment
- Supported

Cyber Essentials / IASME Governance Self-Assessment Service

Provide you with access to 'Pervade' the online IASME Governance Accreditation Scheme Portal. There will be a series of questions that you need to answer that evaluate your basic cyber and information security controls. The areas of your business that will be assessed include;

Cyber Essentials:

- * Organisation
- * Secure Business Operations
- * Access Control
- * User Accounts
- * Malware and Technical Intrusion

IASME Governance:

- * Risk assessment
- * Backup
- * Policies
- * Incident Management
- * Data Protection
- * Operational Management

Cyber Essentials / IASME Governance Supported Service

The "Supported" service gives the same access to the 'Pervade' portal as the Self-Assessment service but also provides you with access to one of our compliance consultants for one-day of consultancy. This can be either attended at your office or delivered remotely.

A reassuringly dull description*



How does it work?

Once your order is received, a member of our customer experience team will take ownership of your order and contact you to introduce themselves as your project lead. They will arrange a Welcome call with you to guide you through the process, outlining who will be responsible for each element of the assessment. We will then:

- Provide access to the Pervade Portal.
- Arrange for the consultancy services (for the Supported service variant).
- Agree a date with you for the assessment.

You will have 6 months to complete your assessment before your account is archived. Upon completion of your question set, one of our auditors will mark your answers to check that the measures you have advised are appropriate. If your application is successful, you will be issued with your certificate.

If you fail to meet the required standard, you are allowed two working days to examine the feedback from the assessor and change any simple issues with your network and policies. You can then update your answers and the assessor will have reassess your submission without further charges. However, if you still fail after these two working days you will be required to reapply and pay the assessment fee again.

Once you successfully achieve your Cyber Essentials / IASME Governance accreditations, this enables you to display your certificate and the logos on your website/marketing material etc.

Normally we require that Cyber Essentials and IASME Governance to be assessed at the same time, but they can be done separately provided that the IASME Governance is completed within 6 months of the Cyber Essentials certification.

Service Availability

The Norm Compliance consultants and Customer Experience teams are available during UK business hours, Monday to Friday 9:00 to 17:30, excluding public holidays.

The Customer Experience team will be on hand to provide technical advice and assistance for any queries or issues should this be required.

A reassuringly dull description*



Cyber Essentials PLUS Service

Cyber Essentials Plus still has the Cyber Essentials simplicity of approach, and the policies and processes required to attain the certification are the same, however for Cyber Essentials PLUS an assessor will carry out a technical audit of your systems to verify the Cyber Essentials controls are in place and working effectively.

This higher level of assurance involves completing the online assessment followed by a technical audit of the systems that are in-scope for Cyber Essentials. This includes a representative set of user devices, all internet gateways and all servers with services accessible to unauthenticated internet users, e.g. a company website.

To obtain the Cyber Essentials PLUS certification, you must have received the accreditation for Cyber Essentials first, whether that is through **norm**, or another certification body. If it has not been done through **norm**, you will be required to provide proof (certificate) that you have obtained Cyber Essentials, so that we can provide the service for Cyber Essentials PLUS. You must have passed your Cyber Essentials within the prior 3 months, in order to be able to undertake the Cyber Essentials PLUS assessment. If your Cyber Essentials certificate was issued more than 3 months prior, you will be required to undertake a new assessment for Cyber Essentials prior to being able to undertake the Cyber Essentials PLUS assessment.

Following confirmation of your valid successful completion of Cyber Essentials certification, a **norm** auditor will visit a representative sample of your offices to complete a technical audit of the systems that are in-scope for your Cyber Essentials Accreditation. Where offices are based internationally or are difficult to access, we may be able to perform this work remotely, where we are able to agree remote access with you.

The assessor will complete the following required tests:

- * Vulnerability Scan of External IP Addresses
- * Authenticated Scan for Device Patching
- * Malware Protection Review
- * Delivery of Malware via Email Review
- * Delivery of Malware via Web Review

How does it work?

Once your order is received, a member of our customer experience team will take ownership of your order and contact you to introduce themselves as your project lead. They will arrange a Welcome call with you to guide you through the process, outlining who will be responsible for each element of the assessment. We will then:

- Confirm your Cyber Essentials certification number and validity. You will need to complete your Cyber Essentials PLUS audit within 3 months of your Cyber Essentials accreditation.
- Arrange a date for the **norm** auditor to review your systems and documentation
- Provide you with a report showing the tests that were carried out and the results of each, including any remedial steps and an overall result advising whether you have been awarded your Cyber Essentials PLUS accreditation.

A reassuringly dull description*



If you fail to meet the required standard, you are allowed two working days to examine the feedback from the assessor and change any simple issues with your network and policies. You can then update your answers and the assessor will have reassess your submission without further charges. However, if you still fail after these two working days you will be required to reapply and pay the assessment fee again.

Once you successfully achieve your Cyber Essentials PLUS accreditation, this enables you to display your certificate and the Cyber Essentials PLUS logos on your website/marketing material etc.

Service Availability

The Norm Compliance consultants and Customer Experience teams are available during UK business hours, Monday to Friday 9:00 to 17:30, excluding public holidays.

The Customer Experience team will be on hand to provide technical advice and assistance for any queries or issues should this be required.

IASME Governance Audited Service

IASME Governance Audited certification is IASME's highest level of certification and is an excellent alternative to ISO 27001 for small and medium-sized organisations. This service aligns with the Government's Ten Steps to Cyber Security and includes the Cyber Essentials certification in addition to controls relating to people and processes. It also covers the General Data Protection Regulation (GDPR) requirements. IASME Governance is aligned to a similar set of controls to ISO 27001 but is more affordable and achievable for small and medium-sized organisations to implement.

To obtain the IASME Governance Audited certification, you must have received the accreditation for Cyber Essentials / ISAME Governance first, whether that is through **norm**, or another certification body. If it has not been done through **norm**, you will be required to provide proof (certificate) that you have obtained, so that we can provide the service for audited service.

The standard includes all of the five Cyber Essentials technical topics and adds additional topics that mostly relate to people and processes, for example:

- * Risk Assessment and management
- * Monitoring
- * Change Management
- * Training and managing people
- * Backup
- * Incident response and business continuity

How does it work?

Once your order is received, a member of our customer experience team will take ownership of your order and contact you to introduce themselves as your project lead. They will arrange a Welcome call with you to guide you through the process, outlining who will be responsible for each element of the assessment. We will then:

- Confirm your Cyber Essentials / ISAME Governance certification number and validity.
- Arrange a date for the **norm** auditor to review your systems and documentation.

The audit involves interviews with members of staff and a review of documentation and system configuration. It does not involve a technical assessment unless you are being assessed to Cyber Essentials PLUS at the same time, although it may be helpful to have technical staff available to provide evidence to the assessor of your system configuration. The audit may include a visit to your HQ office, branch offices or other locations to satisfy the auditor that your good security practices are reflected across the organisation.

- Once the audit is complete, we will provide you with a report showing the questions that were assessed, the tests that were carried out and your results of each question and/or test including any remedial steps, and an overall result advising whether you have been awarded your accreditation.

Once you successfully achieve your IASME Governance Audited accreditation, this enables you to display your certificate and the logos on your website/marketing material etc. The audited certification is renewed

A reassuringly dull description*



at the end of years 1 and 2 by simply renewing the online IASME Governance assessment. At the end of year 3 a full audit, as described above, is required again to renew the certification.

Service Availability

The Norm Compliance consultants and Customer Experience teams are available during UK business hours, Monday to Friday 9:00 to 17:30, excluding public holidays.

The Customer Experience team will be on hand to provide technical advice and assistance for any queries or issues should this be required.

ISO:27001 – GAP Analysis and Readiness Service

ISO 27001 is a specification for an information security management system (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organisation's information risk management processes. This standard enables organisations of any kind to manage the security of assets such as financial information, intellectual property, employee details or information entrusted by third parties.

The ISO:27001 GAP analysis service provides a **norm** compliance specialist to review in-person your current information security posture against the requirements of ISO/IEC 27001. Our **norm** compliance specialist will interview key managers and perform an analysis of your existing information security arrangements and documentation.

The GAP analysis assessment will provide a true picture of your ISO 27001 compliance gap and will include expert advice on how to scope your project and establish your project resource requirements.

Following the assessment, you will receive a gap analysis report of the findings. It will detail areas of compliance and those requiring improvement and provide further recommendations for the proposed ISO 27001 compliance project.

How does it work?

Once your order is received, a member of our customer experience team will take ownership of your order and contact you to introduce themselves as your project lead. They will arrange a Welcome call with you to guide you through the process, outlining who will be responsible for each element of the assessment. We will then:

- Arrange a date for the **norm** auditor to review your systems and documentation.
- Attend your offices and meet with key Stakeholders/Department Heads to advise about the requirements.
- Undertake an ISO:27001 readiness gap analysis to identify the necessary steps required to make your organisation compliant.
- Produce a report containing recommended actions that will need to be completed before the arrangement of your ISO:27001 audit.
- Guide you as required to assist you with completing the recommended actions.
- Undertake a mock audit once the recommended actions have been completed to ensure that your organisation is prepared ahead of your official audit.
- Provide a final brief report that contains the result of your mock audit

Assistance with completing the recommended actions is available on request at an additional charge.

Service Availability

The Norm Compliance consultants and Customer Experience teams are available during UK business hours, Monday to Friday 9:00 to 17:30, excluding public holidays.

The Customer Experience team will be on hand to provide technical advice and assistance for any queries or issues should this be required.