**IASME Certification Guide: Cyber Essentials Plus and IASME Gold**

This detailed guide has been created for organisations that want to work with the Ministry of Justice (MoJ) to provide services or share data.

# Introduction to the Dynamic Framework

Before you bid for a contract with the MoJ, the Dynamic Framework requires all suppliers to obtain cyber security through [Information Assurance for Small and Medium Enterprises (IASME)](https://iasme.co.uk/).

This is to:

* show your commitment to cyber security
* prove that your organisation’s systems can safely handle personal data
* ensure you gain access to government contracts

IASME helps organisations reduce their risks to cyber security, and protect themselves against possible threats.

New suppliers

Applying for IASME accreditation

[Cyber Essentials](https://www.ncsc.gov.uk/cyberessentials/overview) is the government-backed scheme launched in 2014 by [IASME](https://iasme.co.uk/) and the [Information Security Forum](https://www.securityforum.org/).

There are 4 cyber security pathways available under this scheme:

1. Cyber Essentials Basic – the first level of cyber security.
2. Cyber Essentials Plus – a more technical look at your systems.
3. IASME Governance Self-Assessment – an advanced level of verifications.
4. IASME Governance Audited (IASME Gold) – the highest level of cyber security.

You’ll be required to [complete an online assessment](https://getreadyforcyberessentials.iasme.co.uk/questions/) of your organisation’s structure and IT systems. The purpose of the assessment is to help you achieve compliance, so it’s important you provide the correct information.

Things to consider before you apply

The MoJ requires all suppliers to obtain IASME Gold certification in order to bid for contracts.

You can start with the basic version and work your way to IASME Gold. This approach will give your organisation the time to implement the more complex verifications of IASME Gold. However,

You must obtain IASME Gold within 6 months to qualify for contracts with the MoJ. After this time your login details, provided to you on receipt of payment, will expire.

You can bypass the other accreditations and proceed with the highest level of certification. However, you should consider your organisation’s resources before taking this approach. This includes:

* budget
* team (organisation) size and availability
* technical knowledge
* system capabilities

Cyber Essentials Basic

Under the Dynamic Framework, Cyber Essentials Basic as the minimum requirement for all suppliers to win Call-off contracts.

This is a self-assessment option that protects you from the most common cyber threats. Once your assessment is complete, a qualified assessor will verify the information you have provided.

The IT areas covered by Cyber Essentials Basic include:

* firewall protection
* secure configuration
* patch management
* user access control
* malware protection

Certification must be gained at least a month before you intend to begin services with the MoJ.

Get a quote for Cyber Essentials Basic

Cyber Essentials Plus

[Cyber Essentials Plus](https://iasme.co.uk/cyber-essentials/cyber-essentials-plus-find-out-more/) is a more extensive and technical cyber security verification.

This level covers the same IT areas as the basic version, with the exception of your systems and processes being assessed by a [certified body](https://iasme.co.uk/certification-bodies/).

Typically, this will be an onsite audit. However, all assessments are currently being operated remotely. You’ll be notified if this changes.

Get a quote for Cyber Essentials Plus

IASME Governance Self-Assessed

IASME Governance helps you to reach an advanced level of security in a shorter timeframe.

Once you have submitted your online assessment and your answers have been assessed, you’ll be notified within 72 hours if your organisation has passed or failed.

The IT areas covered by IASME Governance include those under Cyber Essentials Plus, as well as:

* General Data Protection Regulation (GDPR) preparation
* risk assessment and management
* people training and management
* change management guidance
* monitoring policies
* a business continuity plan
* an incidence response plan

Get a quote for IASME Governance Self-Assessment

IASME Governance Audited (IASME Gold)

This is the highest level of IASME certification available.

IASME Gold covers the same IT areas as the self-assessed version, with the exception of your systems and processes being assessed by a [certified body](https://iasme.co.uk/certification-bodies/).

Get a quote for IASME Governance Audited (IASME Gold)

IASME Gold suppliers

Implementing technical changes: ‘how to’ guides

You can use the guides below to help you make the key changes and best practice solutions identified during the 'preparation of works’ stage. See The Cyber Essentials 7 Stage Infographic for further details.

You can contact [xxxx@justice.gov.uk](mailto:xxxx@justice.gov.uk) if you’d like to see further guides not included in this list.

How to create an Incident Response Plan

How to write an Intellectual Property Statement

Updating your IT policies

Your organisation will need to develop IT procedures and standards following [IASME Gold](https://iasme.co.uk/iasme-governance/iasme-governance-audited/) certification. This is required for compliance with many information security frameworks that are widely considered as IT best practice.

You can review [example policies](https://redrockconsulting.sharepoint.com/:f:/s/MPS_MoJ/EvnoCdb5FS5DjzuJmqfC6CoBVviYscgbBBhWFF1-Rr1hjg?e=J6glKi) to help you structure your organisational procedures and standards.

You will need to give your employees guidance on how to follow information security policies. This could be in an ‘Information Security Policy’ or employee handbook that requires employees to sign a ‘Policy Acknowledgement Statement’.

You must ensure all employees in your organisation have read and understood these policies.

If you use external IT service providers, you should reference this in the relevant policies so your employees are also aware.

View [example policy templates](https://redrockconsulting.sharepoint.com/:f:/s/MPS_MoJ/EvnoCdb5FS5DjzuJmqfC6CoBVviYscgbBBhWFF1-Rr1hjg?e=J6glKi) for your organisation.

Further support

FAQs

[IASME Cyber Essentials FAQs](https://iasme.co.uk/frequently-asked-questions/)

[NCSC Cyber Essentials FAQs](https://www.ncsc.gov.uk/cyberessentials/faqs)

MoJ contacts

## IASME contacts

[Message IASME](https://iasme.co.uk/contact-us)

Call: 03300 882 752

Email: [info@iasme.co.uk](mailto:info@iasme.co.uk)

Write: The IASME Consortium Ltd

Wyche Innovation Centre  
Upper Colwall  
Malvern  
WR13 6PL

Related links

[Cyber Essentials Plus](https://iasme.co.uk/cyber-essentials/cyber-essentials-plus-find-out-more/)

[Cyber Essentials questions: IASME online assessment](https://getreadyforcyberessentials.iasme.co.uk/questions/)

[Cyber Essentials: requirements for IT infrastructure (PDF)](https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-IT-infrastructure-3-0.pdf)

[Cyber Essentials self-assessment: IASME question booklet (PDF)](https://iasme.co.uk/wp-content/uploads/2021/11/Cyber-Essentials-only-question-booklet_vEvendine.pdf)

[Cyber Essentials scheme (National Cyber Security Centre)](https://www.ncsc.gov.uk/cyberessentials/overview)

[Information Assurance for Small and Medium Enterprises (IASME)](https://iasme.co.uk/)

[Get a quote for Cyber Essentials Plus](https://iasme.co.uk/cyber-essentials/cyber-essentials-plus-get-a-quote/)

[Get a quote for IASME Governance Audited (Gold)](https://iasme.co.uk/iasme-governance/iasme-governance-audited-get-a-quote/)

[IASME Governance Audited (Gold)](https://iasme.co.uk/iasme-governance/iasme-governance-audited/)

[IASME assessment certification bodies](https://iasme.co.uk/certification-bodies/)

[IASME cyber security leadership strategies training (non-technical)](https://iasme.co.uk/cyber-security-leadership-strategies-programme/)

[IASME cyber security leadership strategies training modules (PDF)](https://iasme.co.uk/wp-content/uploads/2020/08/Cyber-Security-Leadership-Strategies-Training-Overview-4.pdf)

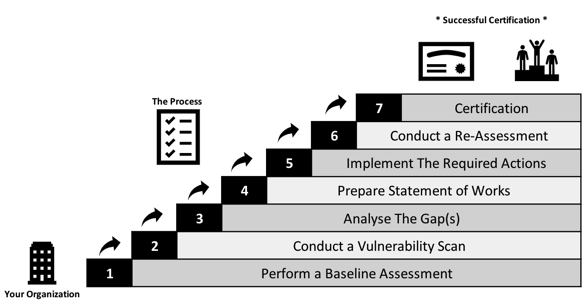
[Minimum Cyber Security Standard (GOV.UK)](https://www.gov.uk/government/publications/the-minimum-cyber-security-standard)

[Small business guide: cyber security (NCSC)](https://www.ncsc.gov.uk/collection/small-business-guide)

[Cyber security: advice for small businesses (GOV.UK)](https://www.gov.uk/government/publications/cyber-security-what-small-businesses-need-to-know)

[Cyber Crime: what is it and how to avoid it (IASME blog)](https://iasme.co.uk/cyber-blog/why-you-need-to-know-about-cyber-crime/)

The Cyber Essentials ~~Plus~~ 7 steps infographic



This is a basic representation of the 7 key steps your organisation will take to obtain the [Cyber Essentials Plus](https://iasme.co.uk/cyber-essentials/cyber-essentials-plus-find-out-more/) certificate.

1. Perform a baseline assessment.
2. Conduct a vulnerability scan.
3. Analyse the gaps (or gaps).
4. Prepare a statement of works.
5. Implement the required actions.
6. Conduct a re-assessment.
7. Certification.

Each step describes what should be done at each stage of the process, and the order to perform them, which is important.