**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.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  | **IASME Certification Paths** |  |
|  | **IT Areas Covered** | **Cyber Essentials** | **Cyber Essentials** **Plus** | **IASME Governance Self-Assessed** | **IASME Governance Audited** **(IASME Gold)** |  |
|  | Firewall | Yes | Yes | Yes | Yes |  |
|  | Secure Configuration | Yes | Yes | Yes | Yes |  |
|  | Patch Management | Yes | Yes | Yes | Yes |  |
|  | User Access Control | Yes | Yes | Yes | Yes |  |
|  | Malware Protection | Yes | Yes | Yes | Yes |  |
|  | GDPR Preparation | No | No | Yes | Yes |  |
|  | Risk Assessment & Management | No | No | Yes | Yes |  |
|  | Training & Managing People | No | No | Yes | Yes |  |
|  | Change Management | No | No | Yes | Yes |  |
|  | Monitoring | No | No | Yes | Yes |  |
|  | Backup & Business Continuity | No | No | Yes | Yes |  |
|  | Incidence Response | No | No | Yes | Yes |  |
|  | Self-Audited | Yes | No | Yes | No |  |
|  | Independently Audited | No | Yes | No | Yes |  |
|  |  |  |  |  |  |  |

Things to consider before you apply

You should choose your certification level and [contact IASME](https://iasme.co.uk/contact-us/) as soon as possible. Covid-19 has caused a significant backlog, which means booking a date with an assessor may take considerably longer.

Ideally, [Cyber Essentials Plus](https://iasme.co.uk/cyber-essentials/cyber-essentials-plus-find-out-more/) must be gained at least one month before you intend to begin services with the MoJ. However, in most cases, the MoJ will require all suppliers to eventually obtain [IASME Gold](https://iasme.co.uk/iasme-governance/iasme-governance-audited/) to bid for contracts.

You can start with [Cyber Essentials Basic](https://iasme.co.uk/cyber-essentials/about-cyber-essentials/) and work your way to [IASME Gold](https://iasme.co.uk/iasme-governance/iasme-governance-audited/) certification. Although, this approach will give your organisation the time to implement the more complex verifications of [IASME Gold](https://iasme.co.uk/iasme-governance/iasme-governance-audited/), it will be more costly.

If you decide to start with the basic version, you must obtain [IASME Gold](https://iasme.co.uk/iasme-governance/iasme-governance-audited/) within 6 months to qualify for contracts. Your login details, provided to you on receipt of payment, will expire after this time.

If you choose to bypass the other accreditations and proceed with the highest level of certification, you should first consider your organisation’s resources. This includes:

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

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.

Cyber Essentials Basic

Under the Dynamic Framework, [Cyber Essentials Basic](https://iasme.co.uk/cyber-essentials/about-cyber-essentials/) is the minimum requirement for 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](https://iasme.co.uk/cyber-essentials/about-cyber-essentials/) include:

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

[Apply for Cyber Essentials Basic](https://iasme.co.uk/cyber-essentials/cyber-essentials-apply-now/)

Cyber Essentials Plus

To qualify for most contracts with the MoJ, [Cyber Essentials Plus](https://iasme.co.uk/cyber-essentials/cyber-essentials-plus-find-out-more/) is the level required to provide services. This level is a more extensive and technical cyber security verification.



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.

[Cyber Essentials Plus](https://iasme.co.uk/cyber-essentials/cyber-essentials-plus-find-out-more/) covers the same IT areas as [the basic version](https://iasme.co.uk/cyber-essentials/about-cyber-essentials/), but your systems and processes are assessed by a [certified body](https://iasme.co.uk/certification-bodies/). This includes looking at:

* a representative set of user devices
* all internet gateways
* all servers with services accessible to unauthenticated users

Typically, this is an onsite audit. However, due to Covid-19, all assessments are currently being operated remotely. You’ll be notified if this changes.

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

IASME Governance Self-Assessed

[IASME Governance Self-Assessed](https://iasme.co.uk/iasme-governance/iasme-governance-self-assessed/) helps your organisation 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 include those under [Cyber Essentials Plus](https://iasme.co.uk/cyber-essentials/cyber-essentials-plus-find-out-more/), 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

[Apply for IASME Governance Self-Assessed](https://iasme.co.uk/iasme-governance/iasme-governance-self-assessed-apply-now/)

IASME Governance Audited (IASME Gold)

This is the highest level of IASME certification. [IASME Gold](https://iasme.co.uk/iasme-governance/iasme-governance-audited/) covers the same IT areas as [the self-assessed version](https://iasme.co.uk/iasme-governance/iasme-governance-self-assessed/), but also includes your systems and processes being assessed by a [certified body](https://iasme.co.uk/certification-bodies/).

You’ll receive 2 quotes from IASME’s assessors, based on the size and complexity of your systems.

This level is a more personalised level of assessment with your chosen assessor. The audit typically involves staff interviews, as well as documentation and system reviews.

Your [IASME Gold](https://iasme.co.uk/iasme-governance/iasme-governance-audited/) certification must be renewed every year, which includes a review of your systems and processes. A full audit takes place every 3 years.

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

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 Plus 7 stage infographic for further details.

You can contact balvinder.naga@justice.gov.uk if you’d like to see further guides not included in this list.

View ‘how to’ guides for support with key tasks.

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/%3Af%3A/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/%3Af%3A/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 contract management

Balvinder Naga, Contracts Manager

balvinder.naga@justice.gov.uk

## IASME

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

Call: 03300 882 752

Email: 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/)