

# Why do Organisations fail Cyber Essentials?



## Andy Lawson CISSP SCCP

Cyber Essentials Technical Assessor (IASME) / MOD Accreditor (DAIS)

NCSC Certified Professional (CCP)

Senior Security & Information Risk Advisor / Senior IA Auditor





Clear statement of basic controls that organisations should implement to mitigate the risk from common internet-based threats.



Mechanism for organisations to demonstrate to customers, investors, insurers and others that they have taken essential precautions against cyber risks.



All new MoD contracts to stipulate that suppliers are Cyber Essentials Scheme compliant.



A set of 5 key controls which will provide cost-effective, basic cyber security for organisations of all sizes:



Secure configuration



Boundary firewalls and internet gateways



Access control and administrative privilege management



Patch management



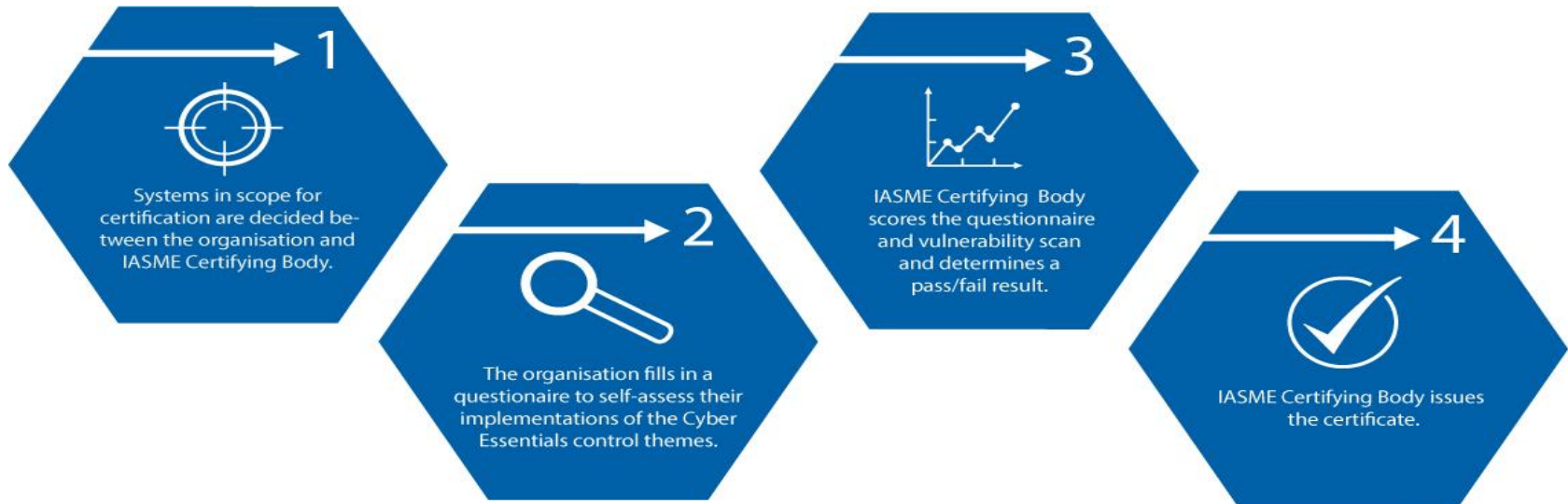
Malware protection

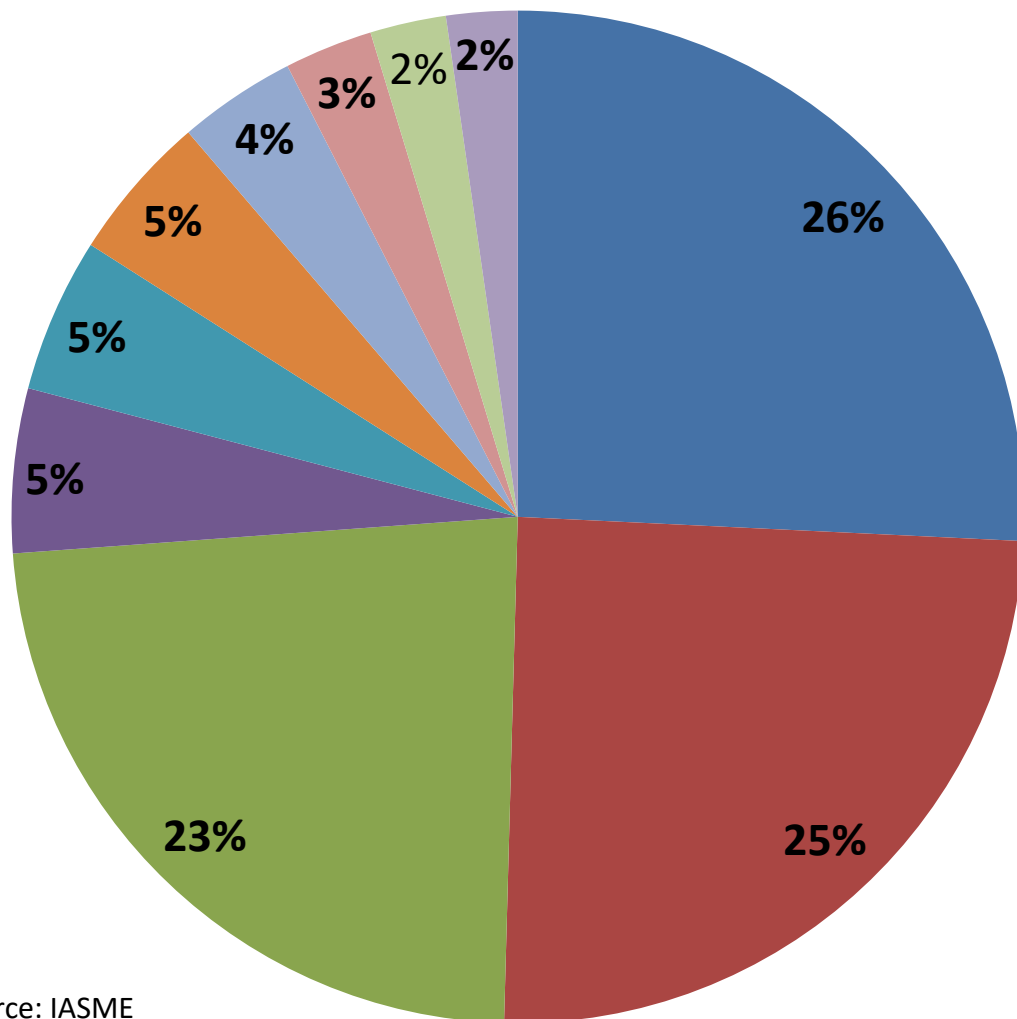
“80% of cyber attacks could be prevented if businesses put simple security controls in place”. (GCHQ, 2015)



## Cyber Essentials (Stage 1).

Certification is awarded on the basis of an independently verified self-assessment. Organisations assess themselves against the five basic security controls.



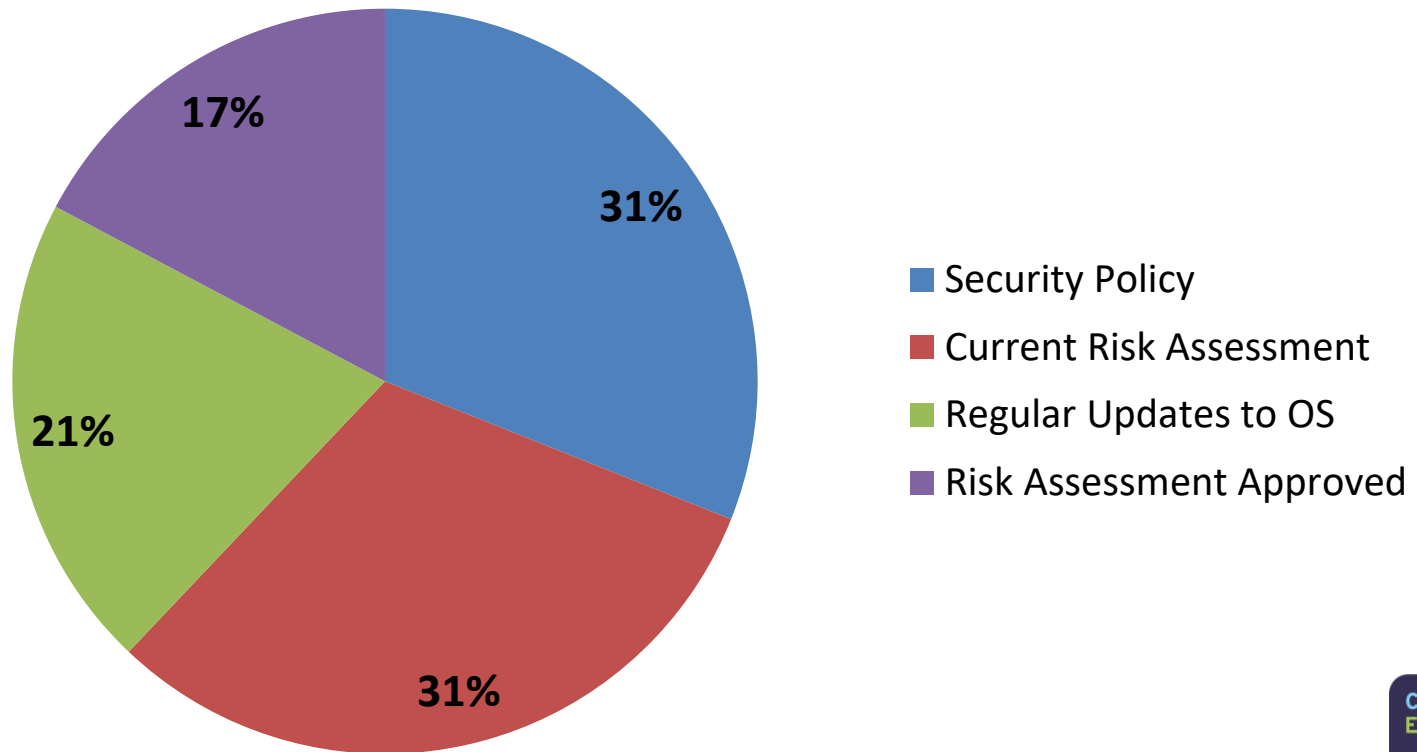


## Top 10 Sectors Using CE

- Professional, scientific and technical
- Information and communication
- Other service activities
- Financial and insurance
- Charity (Registered)
- Manufacturing
- Administration and support services
- Education
- Public administration and defence
- Human Health and Social Work

Source: IASME

## Key Reasons for Automatic Failures

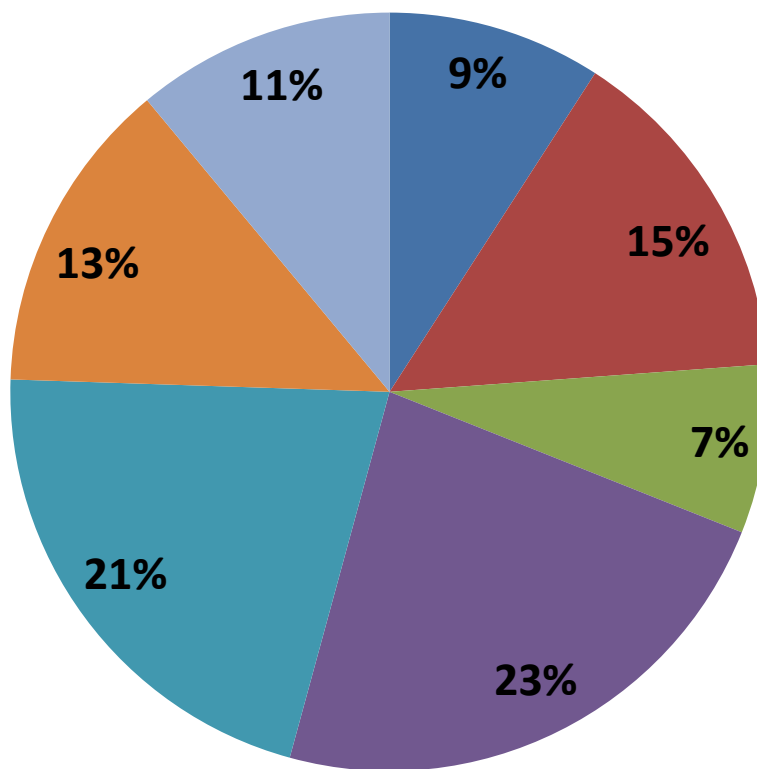


Source: IASME





## Top Non-Compliances

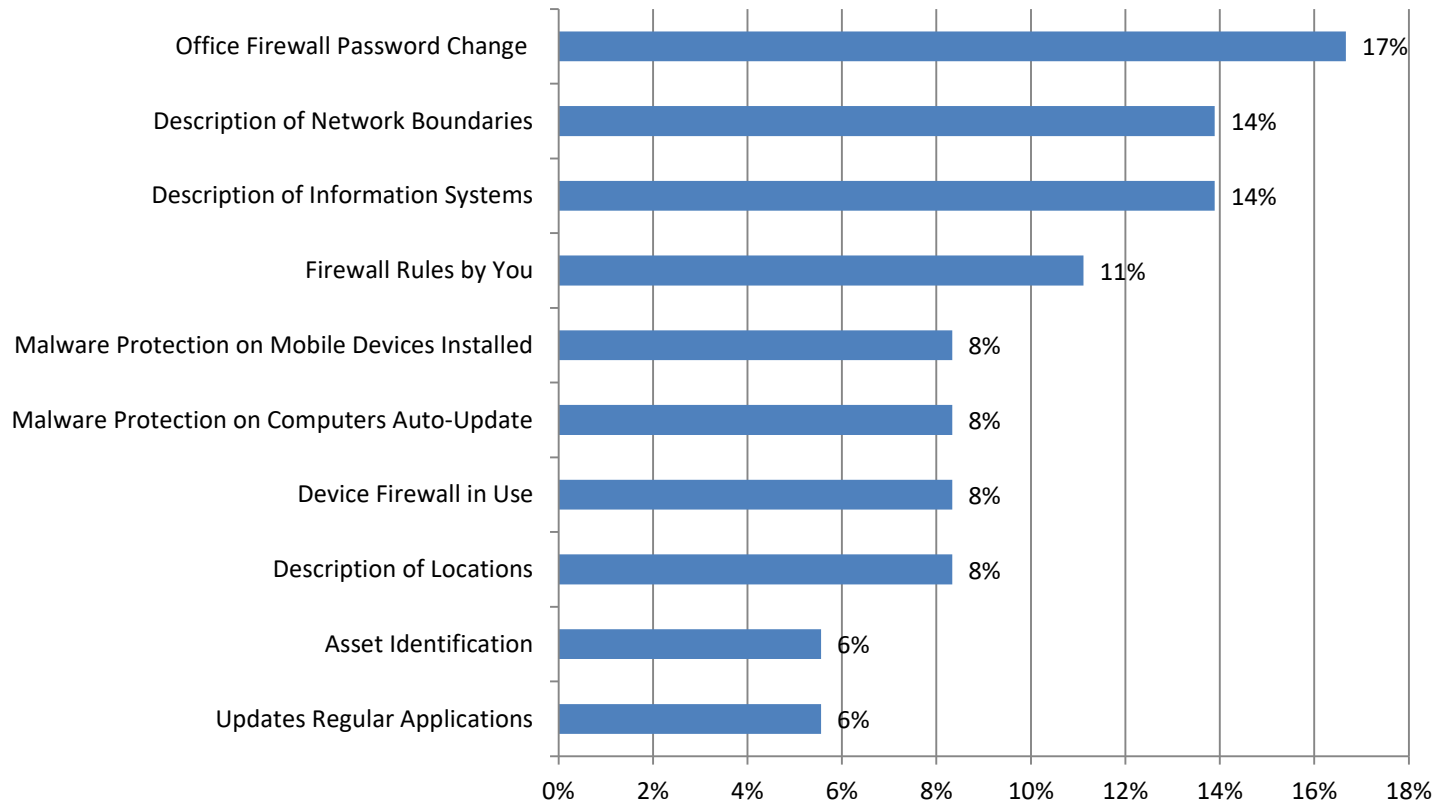


- Malware protection not run daily
- Endpoint malware not run daily
- Firewall passwords not changed regularly
- Admin accounts used day to day
- Admin account password not changed regularly
- 2FA on remote access terminals
- Firewall remote access not accredited

Source: IASME



## Top 10 Common Failure Points





# QUESTIONS ?



# The sales pitch .....

## How to proceed

MASS is an approved Certifying Body with over 30 years of experience providing information systems to government running at the highest security levels. Part of our business is the provision of expert advice around information assurance, direct to businesses and also to the Ministry of Defence.

We offer two fixed price packages for businesses wishing to achieve either Cyber Essentials or Cyber Essentials Plus. A staged flow chart is on the inside of this brochure. If you are interested in discussing your own business' approach to cyber security, and gaining either Cyber Essentials or Cyber Essentials Plus certification, please get in touch with us at [Cyber-Essentials@mass.co.uk](mailto:Cyber-Essentials@mass.co.uk) or using the details below.

We look forward to hearing from you.



Wokingham | PE19 6BN | UK  
[mass.co.uk](mailto:mass.co.uk) | [www.mass.co.uk](http://www.mass.co.uk)  
MCMARKTGIFLY0871

