CYBER EXCELLENCE

BUILDING A SAFER DIGITAL FUTURE FOR THE MIDDLE EAST

ACCREDITED BY

LONDON STRATEGY CENTRE

Developing people and organisations in strategy, innovation and leadership

ASSURED BY

UNIVERSITY OF BIRMINGHAM

TABLE OF CONTENTS

Introduction ____ 04

Why Cyber Excellence? ____ 05

Certification Levels ____ 06

Benefits of Cyber Excellence ____ 07

Timeline ____ 08

Cyber Assessment Framework ____ 09

TABLE OF CONTENTS

Learning from Global Models ____ 10

Message from our Principal ____ 11

Assessment Process By Levels ____ 12

Why Act Now ____ 13

Contact Us ____ 14

CYBER EXCELLENCE

INTRODUCTION

In an era where cyber threats are evolving fast, the Cyber Excellence Certification Scheme stands out as a reliable framework for improving regional cybersecurity. Cyber Excellence is designed to serve organisations of all sizes, from small enterprises and educational institutions to government bodies and critical national infrastructure providers by offering a structured, risk-based approach to certification.

LONDON STRATEGY CENTRE

The London Strategy Centre (LSC) is the Accreditation Body, holding responsibility for the ownership and maintenance of the certification framework. LSC operates to the highest standards of competence and impartiality. The centre liaises with governments, industry stakeholders, and international partners to align the framework with regulatory requirements and sector-specific needs. Its leadership role ensures that the framework meets compliance standards and drives strategic alignment between cybersecurity readiness and national digital transformation agendas.

UNIVERSITY OF BIRMINGHAM

Birmingham University acts as the independent Assurance Body for this Cybersecurity Certification Framework. It ensures the integrity of the scheme and the drives continual improvement. This includes conducting impartial reviews of certification activities, analysing certification trends, and generating threat insights that feed back into the framework's evolution. Through its global academic expertise, the Assurance Body provides evidence-based oversight and ensures that the certification process remains rigorous, credible, and aligned with international best practices.

WHY CYBER EXCELLENCE?

A REGIONAL SOLUTION FOR A REGIONAL CHALLENGE

As the Middle East continues to rely more and more on digital platforms, tough cybersecurity measures are not only a business necessity but also a regulatory requirement. The region faces escalating cyber risks that impact organisations across both the public and private sectors. Cyber Excellence was established to address these local challenges, aligning its certification model with regional frameworks such as the Saudi National Cybersecurity Authority (NCA). Essential Cybersecurity Controls (ECC), the UAE Information Assurance Standards (IAS), and the Gulf Cooperation Council (GCC) Cybersecurity Strategy. By harmonising with these and other national mandates, Cyber Excellence ensures that certification is regionally relevant and internationally credible.

CERTIFICATION LEVELS

With “Cyber Excellence , organisations in all sectors can scale securely, governments can ensure robust supply chains, and the Region can move towards unified cybersecurity standards aligned with digital transformation.”

ENTRY LEVEL

Self-assessment for low-risk organisations.

FOUNDATION LEVEL

Additional controls for low-risk organisations.

CERTIFIED LEVEL

Independent assessment for moderate-risk organisations.

ASSURED LEVEL

Highest standard for critical infrastructure.

BENEFITS OF CYBER EXCELLENCE

COMPLIANCE

Align with key national regulations, including NCA ECC, UAE IAS, ensuring regulator and partner confidence.

RISK REDUCTION

Apply controls addressing most regional threats, including those flagged by ARCC and local intelligence.

TRUST

Prove proactive data protection and resilience through independent assessment recognised across Middle Eastern markets.

RESILIENCE

Certified controls help prevent, detect, and respond to cyber threats, ensuring business continuity.

CREDIBILITY

Certification demonstrates strong cybersecurity commitment, boosting trust with customers, partners, and investors.

ADAPTABILITY

Cyber Excellence certification evolves with threats, supporting growth and digital transformation.

TIMELINE

1971

The first known computer virus, Creeper, is created as an experiment.

1983

The term “cybersecurity” is first used.

2007

CITC launches Computer Emergency Response Team (CERT)

2012

First formal National Cybersecurity Strategy was introduced to improve governance.

2017

Establishment of the National Cybersecurity Authority (NCA)

Present

Persistent cyber threat landscape.

CYBER ASSESSMENT FRAMEWORK

We follow the UK’s NCSC Cyber Assessment Framework (CAF), taking a systematic and comprehensive approach to assessing how effectively the organisation responsible is managing cyber risks to essential functions.

NCSC CYBER ASSESSMENT FRAMEWORK

Minimising Impact of Incidents

Centers on response planning and learning from past incidents to reduce future damage.

Managing Security Risk

Use governance, risk, asset, and supply chain management to mitigate potential threats.

Detecting Cybersecurity Events

Security monitoring and threat hunting to identify and address security incidents.

Protecting Against Cyber Attack

Service protection, identity control, data security, and staff training to prevent breaches.

LEARNING FROM GLOBAL MODELS

99%

of internet-based vulnerabilities mitigated with certified controls.

82%

of certified organisations reported improved confidence in defending against threats.

61%

of buyers prefer certified suppliers.

71%

of organisations see improved executive engagement with cybersecurity.

A leading UK wealth management firm, mandated certification for its partner network. Within a year, this initiative resulted in:

80% reduction in cyber incidents among certified partners.

A unified assurance standard across thousands of suppliers.

Simplified compliance via independent certification.

Cyber Excellence adapts these lessons for the Middle East, ensuring both small and large organisations benefit from a cohesive framework.

Cyber Essentials Impact Evaluation (2024), Department for Science, Innovation and Technology (DSIT).

MESSAGE FROM OUR PRINCIPAL

"In cybersecurity, standing still is falling behind. Regular reassessment and updated certification standards create a culture of vigilance, ensuring teams remain aware and proactive. Continuous improvement isn't optional, it's the only way to stay ahead of evolving threats and protect critical assets in an ever-changing digital landscape."

MAJOR GENERAL PAUL NANSON

Principal, London Strategy Centre

ASSESSMENT PROCESS BY LEVELS

ENTRY LEVEL 1

HOW IT'S ASSESSED

Self-assessment via a short online questionnaire.
Light-touch independent verification of declarations.
Scope: Five core technical controls (Cyber Essentials-aligned):

- Firewalls & internet gateways
- Secure configuration
- User access control
- Malware protection
- Patch management

FOUNDATION LEVEL 2

HOW IT'S ASSESSED

Includes all Level 1 aspects.
Independent technical verification by a qualified assessor, including:

- External/internal vulnerability scanning
- Checks for unpatched/misconfigured systems
- Malware/AV effectiveness checks
- User device build reviews (laptops, desktops, mobiles)
- Tests confirming boundary and access control measures

CERTIFIED LEVEL 3

HOW IT'S ASSESSED

Includes all Level 1 & 2 assessment activities.

- Deeper sampling and evidence review (policies, runbooks, intrusion prevention configs, backup/restore records).
- Effectiveness validation (tabletop exercises, restore tests, incident response walkthroughs).
- Supplier oversight checks (contracts, SLAs, assurance artefacts).

ASSURED LEVEL 4

HOW IT'S ASSESSED

Includes all Level 1–3 activities.

- Threat-led testing (e.g., red/purple teaming, breach & attack simulation) mapped to crown-jewel assets.
- Architecture & design assurance (network segmentation, zero-trust patterns, high-availability and failover).
- Operational resilience validation (RTO/RPO evidence; crisis exercises with executives).
- Continuous monitoring and SOC use-cases with measurable detection /response SLAs.
- Metrics & governance reviewed at board level; transparent reporting to regulators where required.

WHY ACT NOW

PROVEN IMPACT

Cyber Excellence builds on trusted international models like NIST, Cyber Essentials and IASME Cyber Assurance, ensuring globally recognised best practices are applied locally.

COMMERCIAL ADVANTAGE

Achieving Cyber Excellence certification demonstrates compliance with key client and regulatory requirements ahead of competitors. This strengthens market positioning and opens doors to new business opportunities and high-value contracts.

SCALABLE APPROACH

Cyber Excellence is designed to be accessible to organisations of all sizes, from SMEs to critical infrastructure operators. Its adaptable framework allows businesses to start small and expand their cybersecurity maturity as they grow.

CULTURAL CHANGE

Certification shifts cybersecurity from being an IT issue to a core business priority. By capturing executive attention, it embeds security into everyday decision -making and operational processes.

Cyber Excellence Level 1 is recommended as a minimum standard of cybersecurity that every organisation - no matter its size - should aim for.

To find out more about our certifications or to have a conversation with one of our experts about how we can support you, please visit our website **londonstrategycentre.com**

CONTACT US

www.londonstrategycentre.com

London Strategy Centre

Cyberexcellence@londonstrategycentre.com

43 Upper Grosvenor St London, W1K 2NJ, United Kingdom

ACCREDITED BY

LONDON STRATEGY CENTRE
Developing people and organisations in strategy, innovation and leadership

ASSURED BY

UNIVERSITY OF BIRMINGHAM