



ISACA®



CMMI® Institute

# **CMMI-BASED** **guidance for** **the UK** **CYBER** **GOVERNANCE** **CODE OF** **PRACTICE**



**demix**™  
Create | Evolve | Perfect



**Excellence** in  
**Measurement**  
**Technology**



# INTRODUCTION: LEADING CYBER RESILIENCE FOLLOWING CMMI

---

In today's digital economy, cyber resilience is a board-level imperative

The UK government introduced the Cyber Governance Code of Practice on 8 April 2025 to strengthen organisational oversight of cyber risk. The Code outlines critical governance actions for boards and directors to manage digital risks and protect against cyber attacks. It forms part of a wider governance package, supported by free NCSC resources: Cyber Governance Training (board responsibilities) and the Cyber Security Toolkit for Boards (practical guidance).

To translate these expectations into actionable, sustainable, and auditable practices, organisations benefit from a robust process improvement framework. CMMI (Capability Maturity Model Integration) helps boards and executives turn high-level governance intent into day-to-day behaviours, controls, and measurable outcomes that align with the Code.

This brochure demonstrates how CMMI may be used to support the implementation of the UK Cyber Governance Code of Practice—providing a structured path from policy to practice, with measurable, repeatable, and scalable outcomes for boards and organisations.

CMMI is a globally recognised model for enhancing performance across engineering and service delivery. Used alongside the Code, CMMI provides a flexible, outcomes-driven approach to reduce risk, improve process capability, and deliver repeatable, resilient cybersecurity results.

# CMMI & THE UK CYBER GOVERNANCE CODE OF PRACTICE

The Cyber Governance Code of Practice is designed for organisational leaders in establishing an environment for effective cybersecurity and resilience. It outlines **five critical governance domains** to ensure cyber risk is managed as a strategic business issue.

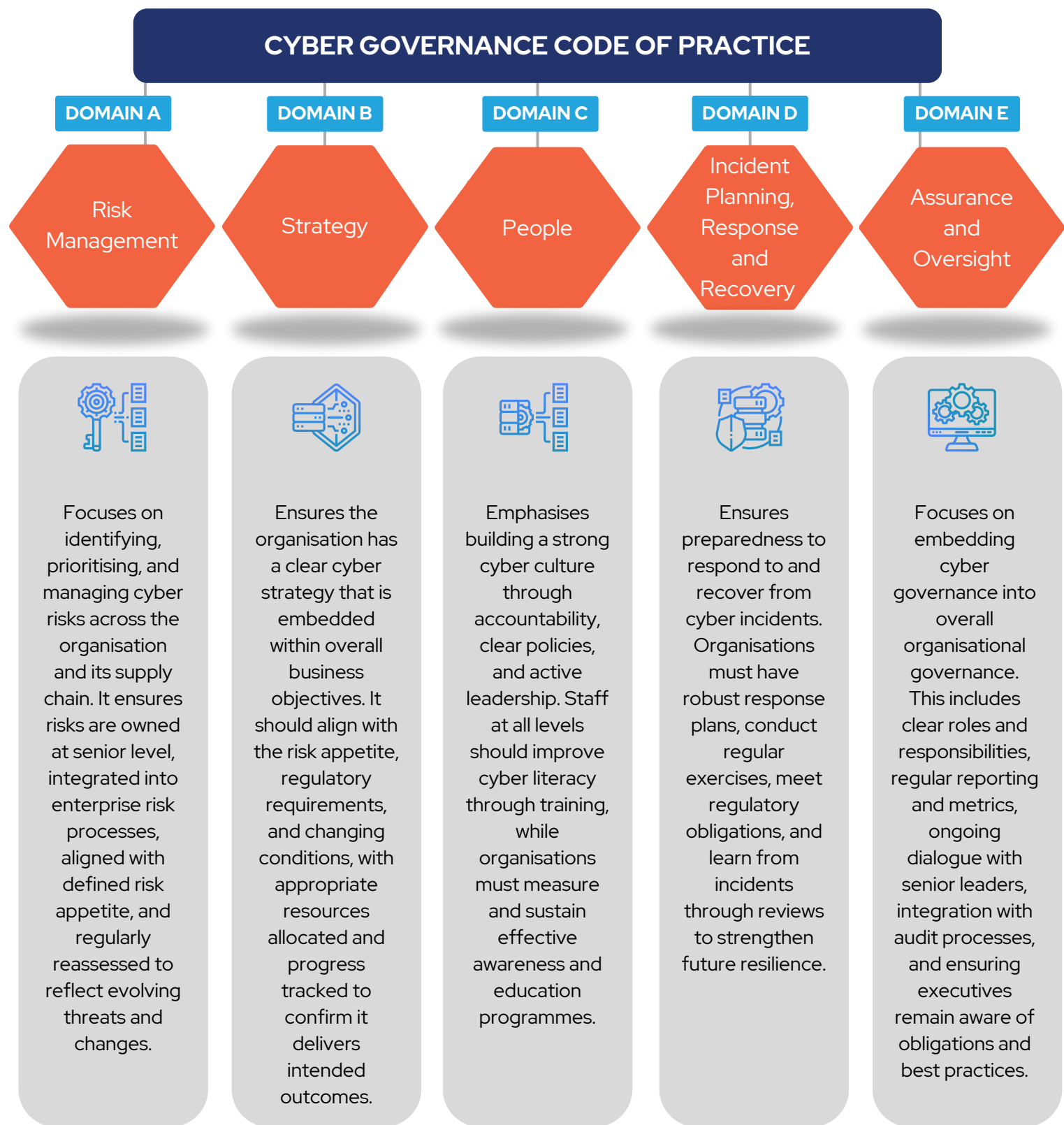
The table below provides **examples** of how **CMMI** provides the operational backbone to turn governance expectations into actions.

Domain	Action		Mapped CMMI V3.0 PAs (Practice Areas)	Example Implementations Using CMMI Practices
Strategy	B1	Gain assurance that the organization has developed a cyber strategy and this is aligned with, and embedded within, the wider organizational strategy	Enabling Security (ESEC), Managing Security Threats and Vulnerabilities (MST)	<p>The organisation engages all relevant security stakeholders to document and implement a cybersecurity strategy that:</p> <ul style="list-style-type: none"><li>• Defines security policies, and functional responsibility for maintaining cybersecurity;</li><li>• Identifies common attack vectors, threat agents and patterns of attack;</li><li>• Defines a security architecture to address common threats;</li><li>• Identifies process controls for managing vulnerabilities;</li><li>• Determines mechanisms, and roles and responsibilities for addressing security events;</li><li>• Provides policies for adopting or meeting the challenges of evolving technologies (e.g. AI)</li></ul>

Domain	Action		Mapped CMMI V3.0 PAs (Practice Areas)	Example Implementations Using CMMI Practices
Incident Planning, Response and Recovery	D1	Gain assurance that the organisation has a plan to respond to and recover from a cyber incident impacting business critical technology processes, information and services	Continuity (CONT), Incident Resolution & Prevention (IRP), Enabling Security (ESEC), Managing Security Threats & Vulnerabilities (MST), Risk & Opportunity Management (RSK)	<ul style="list-style-type: none"> <li>The organisation clearly documents and implements a Security Incident Handling process that includes: <ul style="list-style-type: none"> <li>Assigning ownership based on severity;</li> <li>Mechanisms for escalation;</li> <li>Mechanisms for notifying affected stakeholders;</li> <li>Eradicating causes of security incidents;</li> <li>Restoring operations; and</li> <li>Learning lessons and identifying security improvements</li> </ul> </li> <li>Business Continuity Plans are in place that: <ul style="list-style-type: none"> <li>Identify key functions, infrastructure and data;</li> <li>Identify mechanisms for their backup, restoration, recovery or replacement.</li> </ul> </li> <li>Business Continuity Plans are regularly tested to validate their effectiveness <ul style="list-style-type: none"> <li>E.g. security drills, simulations, and tabletop exercises.</li> </ul> </li> </ul>

**CMMI TURNS INCIDENTS INTO OPPORTUNITIES FOR IMPROVEMENT.**

# OVERVIEW OF CODE OF PRACTICE



# WHY CMMI? THE STRATEGIC ADVANTAGE

CMMI is not just a process model, it is a strategic enabler for cybersecurity excellence. By leveraging CMMI, organisations can:

1

**Demonstrate a structured way to address UK codes of practice using well recognised best practices**

2

**Integrate security into core business processes, not as an afterthought**

3

**Empower leadership with data-driven insights and accountability mechanisms**

4

**Build customer trust through transparency, resilience, and consistent delivery**

5

**Future-proof operations against evolving threats and regulatory expectations**

CMMI's modular, context-specific design allows organisations to tailor the model to their unique needs, whether agile, waterfall, or hybrid. It supports integration with other standards like ISO 27001, NIST, and ITIL, making it a unifying framework for performance improvement.

# NEXT STEPS: BUILDING YOUR CYBER- RESILIENT ORGANISATION

1. Learn more about the CMMI model by attending a Building Organizational Capability (BOC) course
2. Assess your current maturity against CMMI and the UK Cyber Governance Code of Practice
3. Align your secure development, governance, and operations practices with CMMI
4. Implement targeted improvements using CMMI's structured guidance
5. Validate through internal assessments or third-party evaluations
6. Communicate your commitment to customers, regulators, and stakeholders


## SUPPORTING RESOURCES

### 01.

#### CMMI RESOURCES AND TRAINING

##### **Excellence in Measurement**

→ [www.excellenceinmeasurement.com](http://www.excellenceinmeasurement.com)

kieran.doyle@eximt.com 

##### **Demix**

→ [www.demix.org](http://www.demix.org)

info@demix.org 

##### **CMMI Institute**

→ [www.cmmiinstitute.com](http://www.cmmiinstitute.com)

### 02.

#### UK GOVERNMENT GUIDANCE

[Cyber Governance Code of Practice](#)



FIND OUT MORE 