ISACA

CMMI® Institute

CMMI-BASED guidance for the UK SOFTWARE SECURITY CODE OF PRACTICE

demix™
Create | Evolve | Perfect

Excellence in Measurement Technology

Prepared by Demix and Excellence in Measurement and Technology

VERSION 4

INTRODUCTION: LEADING CYBER RESILIENCE FOLLOWING CMMI

In today's digital economy, cyber resilience is a strategic imperative

The UK government has introduced the Software Security Code of Practice to strengthen organisational security. This code of practice was published 7 May 2025. This framework guides software vendors in building, maintaining, and distributing secure software by setting clear technical and operational expectations for secure delivery.

To turn these principles into actionable, sustainable, and auditable practices, organisations need a robust process improvement framework. CMMI (Capability Maturity Model Integration) provides exactly that.

CMMI is a globally recognised model for enhancing performance across engineering and service delivery. Developed by industry experts, CMMI is not a checklist — it is a flexible, outcome-driven ecosystem designed to help organisations improve capability, reduce risk, and deliver value. By adopting CMMI's best practices to support the Software Security Code, organisations can move beyond compliance to achieve measurable, repeatable, and resilient cybersecurity outcomes.

This brochure demonstrates how CMMI may be used to support the implementation of the UK Software Security Code of Practice—providing a structured path from policy to practice, with real-world relevance and scalability.

CMMI & THE UK SOFTWARE SECURITY CODE OF PRACTICE

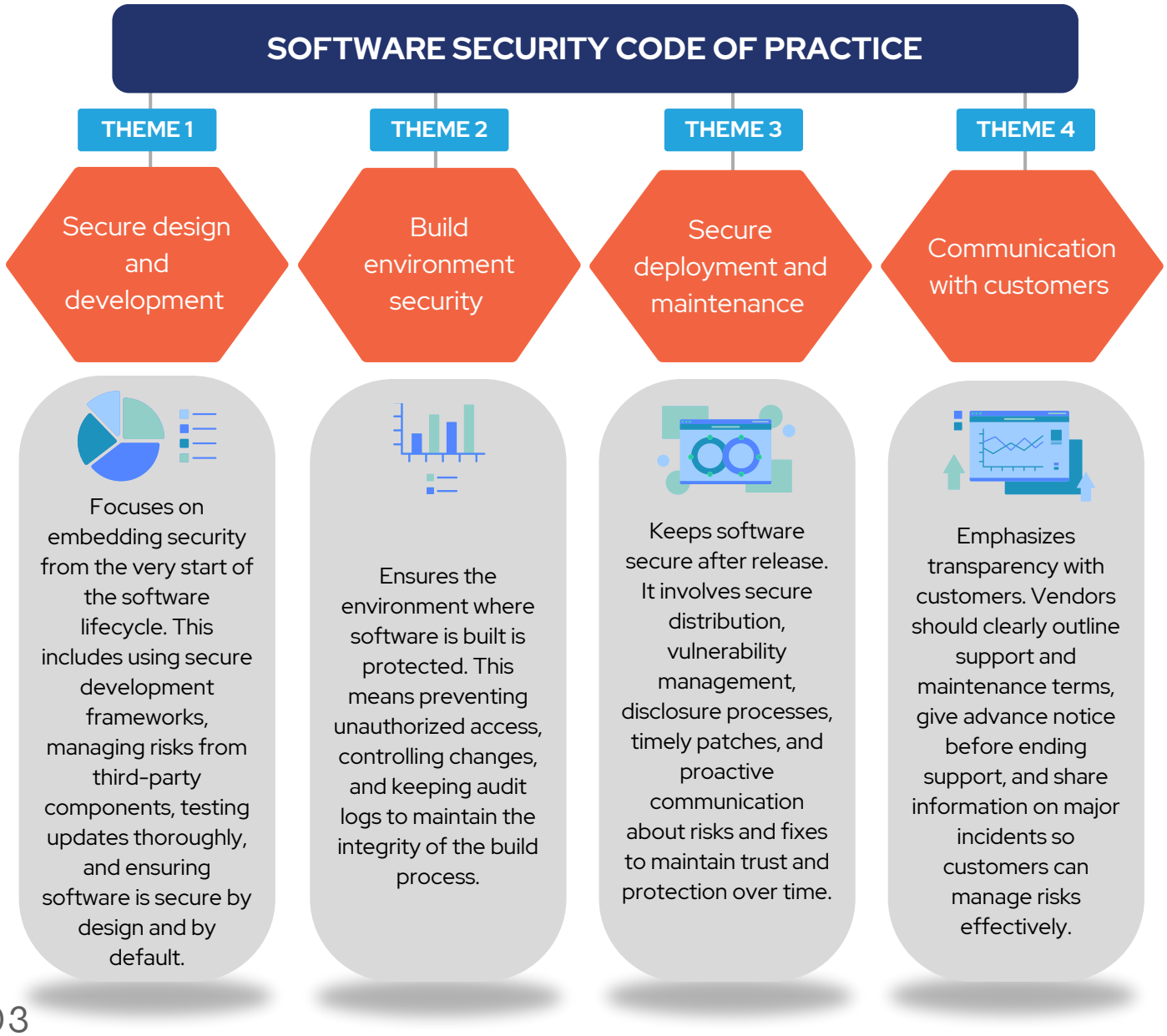
The Software Security Code of Practice outlines **14 principles** across **four themes** to help software vendors reduce supply chain risks and strengthen software resilience. Currently no formal mapping exists between the Software Security Code of Practice and CMMI practices.

However, the table below demonstrates using a couple of **examples**, how the principles may be addressed using the best practice encapsulated in **CMMI** practices.

Theme	Principle		Example Implementations Using CMMI Practices
1. Secure design and development	1.4	Follow secure by design and secure by default principles throughout the development lifecycle of the software	As part of the strategy for addressing this principle, the organisation defines and monitors usage of design criteria and methodologies to be applied in guiding design decisions for the organisation's products: • Conduct Threat Modelling. • Use established design patterns. • Adopt secure design principles, for example: ◦ Build defence in depth, layering security; ◦ Grant only necessary access privileges; ◦ Incorporate secure defaults that ensure the product is "safe out-of-the-box." • Review designs for acceptable organisational levels of: ◦ Complexity; ◦ Scalability; ◦ Usability; ◦ Maintainability.

Theme	Principle		Example Implementations Using CMMI Practices
2. Build environment security	2.1	Protect the build environment against unauthorised access	The organisation defines and enforces a strict policy in regards of tools and environments that may be used in development work. This may extend to the adoption of Security Technical Implementation Guides (STIGs) in the design of corporate networks. The environments are subject to regular security and configuration audits.

The figure below demonstrates
the 4 themes of the software security 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 Software Security 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

Demix

→ www.demix.org

info@demix.org

Excellence in Measurement

→ www.excellenceinmeasurement.com

kieran.doyle@eximt.com

CMMI Institute

→ www.cmmiinstitute.com

02.

UK GOVERNMENT GUIDANCE

Software Security Code of Practice

FIND OUT MORE