Grant Thornton
An instinct for growth™

Information Security

C2M2

The Cybersecurity Capability Maturity Model

January 2018

3502GT-01-18

What is C2M2?

C2M2 was devised by the US Department of Energy (DoE) to evaluate and improve information security in the electricity sector. The model is in the public domain, and so any organisation is free to use it to understand its maturity with regard to information security.

Why is it relevant to me?

A C2M2 assessment provides a comprehensive, manageable description of your organisation's information security. It assesses the maturity of your information security in ten distinct categories (termed "domains"), and clearly illustrates any areas that require improvement. Additionally, the outputs of a C2M2 assessment provide a valuable foundation if you are considering adopting one of the many formal information security standards such as ISO 27001 or the NIST Cybersecurity Framework, as the content of C2M2 correlates well with these other standards.

What does a C2M2 rating look like?

C2M2 assesses approximately 300 controls, split across the ten domains. Each control has a Maturity Indicator Level, or MIL, which is a measure of the control's significance. For instance a MIL1 (low level) control may relate to the basic existence of a person to whom information security incidents are reported; while a MIL3 (high level) control may be a more specific regime where incidents are reported to and co-ordinated with third parties.

Each control is scored with one of four classifications:

- **Not Implemented:** There is no evidence of the control being implemented.
- **Partially Implemented:** There is some evidence of relevant activity, usually on an ad-hoc basis.
- **Largely Implemented:** Clear evidence exists that controls are in place and used by a significant number of staff.
- **Fully Implemented:** Strong controls are fully embedded within the day-to-day operation of the organisation.

The 10 C2M2 domains

- Risk Management
- Asset, Change, and Configuration Management
- Identity and Access Management
- Threat and Vulnerability Management
- Situational Awareness
- Information Sharing and Communications
- Event and Incident Response, Continuity of Operations
- Supply Chain and External Dependencies Management
- Workforce Management
- Cybersecurity Programme Management

How Grant Thornton can help

The C2M2 model is freely available and is designed as a self-assessment tool: as such, there is no obligation to engage an outside agency for C2M2 assessments. Practically speaking, though, the model is lengthy and engaging a third party with experience in C2M2 assessments and remediation will generally save time and improve quality, as well as providing an impartial evaluation of your maturity. Our information security specialists will work with you to:

- Evaluate your organisation's capabilities within the ten domains of the C2M2 model and produce a comprehensive report of findings.
- Identify and prioritise areas for improvement and the actions required.
- Design and, if required, manage the programme of actions.
- Re-evaluate your capabilities regularly (normally annually) to monitor information maturity security over time.

For more information please contact:

David Cartwright
Senior Consultant, Information Security
T +44 (0) 1534 885813
E david.cartwright@gt-ci.com

Grant Thornton

An instinct for growth™

grantthorntonci.com