MICROPOLE

Towards a Pragmatic Cyber Strategy

Why Start with C2M2 before CIS CSC and Risk Analysis?

2023

From maturity to risk, through controls, programs and back.

editors

JÉRÔME DOSSOGNE

Cybersecurity Service Manager

Yes «change is permanent, inevitable, natural.» We all have been told that over and over. «Nothing lasts forever.»

But...experience has shown us, again and again, that a cultural migration is by no means easy to perform nor will it «naturally» lead to the optimal result, even under very reasonable and pragmatic assumptions.

The guidance frameworks offer in a chaotic world should not be seen as a desire to ignore an organization's uniqueness and necessities. We believe the aim should be to address and bridge both technical challenges and managerial challenges keeping a down to earth, pragmatic approach and staying true to the organization's uniqueness.

BENOIT TANCREDI

Partner &
Director Cybersecurity Services

The implementation of a cybersecurity framework should not just be about compliance; it should be a strategic initiative that brings measurable value by substantially elevating the security landscape of the organization.

A holistic cycle

In the ever-changing landscape of cybersecurity, taking a holistic approach to protect organizations from constantly evolving threats has become imperative.

This is not an area where a single framework can offer a complete solution. Or at least, from experience, such attempts to cure all ills at once with a single bullet too often leads to unsatisfactory results.

Effective cybersecurity often results from harmonizing various types of approaches and therefore, best practices frameworks; taking advantages of what each has to offer and focusing on their specific aim (see Fig. 1):

- **maturity** frameworks like **DoE/DHS's C2M2** for assessing current capabilities,

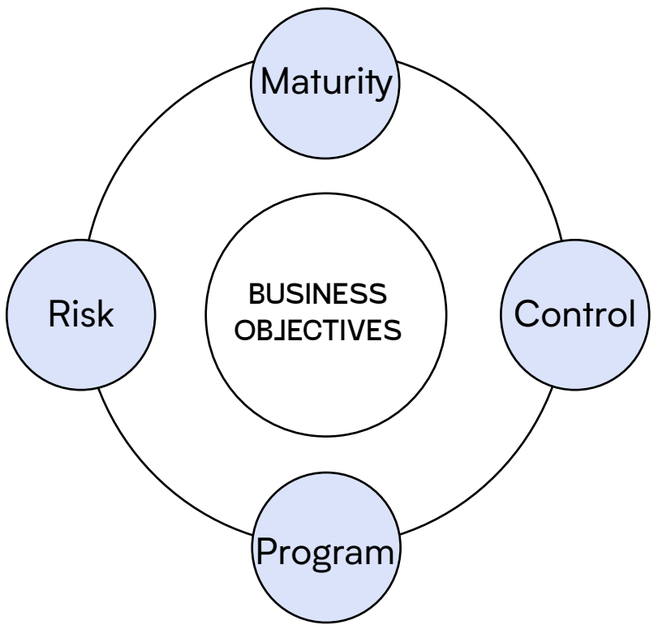
- **control** frameworks like **CIS CSC, NIST SP800-53 and ISO 27002** for immediate actions,

- **program** frameworks like **NIST CSF** and **ISO 27001** for organizational structure,

- and **risk** management frameworks like **NIST RMF (SP800-30,37,39), ISO 27005 and FAIR** for in-depth multi-factorial assessments.

Fig. 01

Cyber security frameworks in balance



Dodging the paralysis

From multinationals to SMEs, and even governmental institutions, no one is immune to cyber threats. Yet, while the need to protect oneself becomes increasingly clear, **the «how» often remains elusive.**

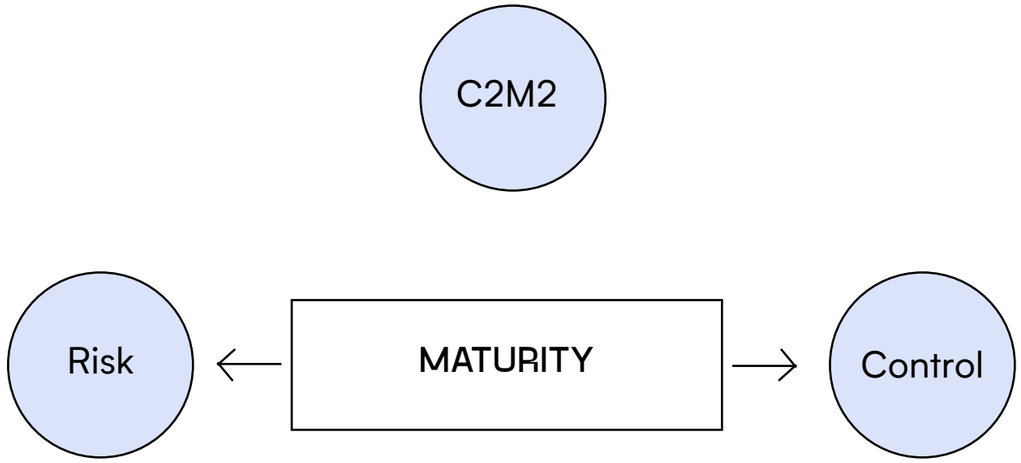
Traditionally, the starting point for securing an organization has been a comprehensive risk analysis which leads to "Top-Down" analysis. While important, these analyses can be timeconsuming, resource-intensive, and more often than none, very complex.

This complexity often leads to «paralysis by analysis»—the inability to act due to information overload as much as information scarcity/ unavailability.

This is where maturity frameworks, such as the DoE/DHS C2M2 (Cybersecurity Capability Maturity Model), offers a more accessible entry point. It allows organizations to assess their existing cybersecurity capabilities, making it easier to identify gaps and prioritize actions. (Fig. 2)

Fig. 02

C2M2 as a driver to the right approach



With a foundational understanding through C2M2, organizations are better equipped to adopt **pragmatic and immediately actionable measures,** like those offered by the Center for Internet Security's 18 Critical Security Controls and the ISO/IEC 27002. To streamline this process further, there's the CSAT (CIS Security Assessment Tool), designed to help organizations identify gaps in the implementation the CIS CSC controls more efficiently. (fig.3)

Additionally, the ISO/IEC 27002 extends that list of controls and allow to offer a different perspective to help ensuring that all the reasonable bases have been covered as per industry standards.

Fig. 03

CIS Security assessment tool

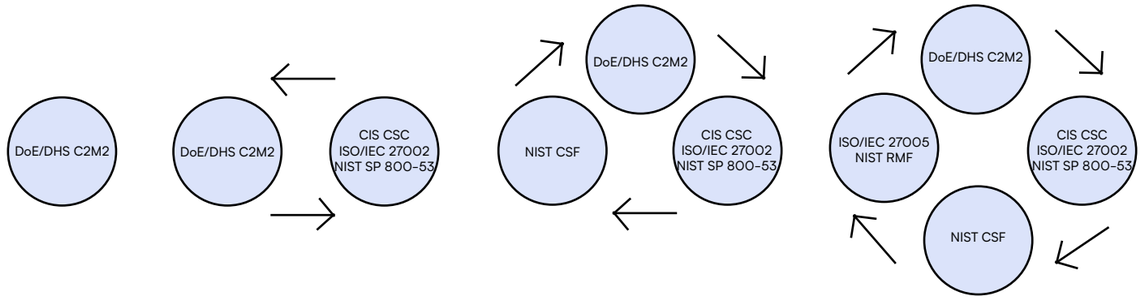
The cycle of (cyber) life: evolving step by step

One often-overlooked feature is the cyclic nature of frameworks. Once initial controls are established, organizations aren't left to fend for themselves.

They need to maintain and, on regular interval, reassess their security posture, fine-tune their controls, and integrate and extend their analysis with other frameworks, models and sets of recommended controls, activities for a more robust strategy. (fig. 4)

Fig. 04

CIS Security assessment tool



Of course, there are various types of frameworks aside from DoE/DHS C2M2 and CIS CSC. While DoE/DHS C2M2 focuses on assessing the maturity of an organization's cybersecurity capabilities, program frameworks help establish the structure and processes required to manage cybersecurity initiatives. Starting with C2M2 as a foundational assessment, then moving on to CIS CSC for control implementation, followed by programs and risk frameworks, enables the seamless integration of these other frameworks, **resulting in a comprehensive cybersecurity strategy.**

The seeming simplicity of starting with maturity frameworks, such as DoE/DHS C2M2, and then advancing to control frameworks, such as CIS CSC, doesn't compromise effectiveness. In fact, i**t allows businesses to first gauge their cybersecurity maturity and then focus on essential controls** extending on those with ISO/IEC 27002 and freeing up resources for more complex initiatives like incorporating additional frameworks such as developing their program with the NIST CSF and integrating all the aspect of the organizations from threats, vulnerability to impact with a risk framework.

In an ideal world, every organization would have the resources and capability to efficiently use a "Top-Down" approach with the conduct detailed risk analyses from the start. However, reality is often less than ideal. For many organizations, particularly smaller ones, a pragmatic approach based on maturity (C2M2), followed by controls (CIS CSC) and corresponding support tools (CSAT), **offers a quicker and more cost-effective path to achieving an acceptable level of cybersecurity**.

Would you like to know how your organization can get started?

FRAMEWORK REFERENCES

This whitepaper is based on the following references, that are publicly accessible via the links prodived below:

1. CIS CSC https://www.cisecurity.org/controls
2. DoE/DHS C2M2 https://c2m2.doe.gov/
3. ISO/IEC 27002:2022 https://www.iso.org/standard/75652.html
4. ISO/IEC 27005:2022 https://www.iso.org/standard/80585.html
5. ISO/IEC 27001 https://www.iso.org/standard/27001
6. FAIR https://www.fairinstitute.org/
7. NIST SP800-53 https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
8. NIST CSF https://www.nist.gov/cyberframework
9. NIST RMF https://csrc.nist.gov/projects/risk-management/about-rmf

LEGAL INFORMATION

EDITORS: Benoit Tancredi, Jérôme Dossogne

Copyright ® 2023 Micropole, Cybersecurity Services CoE

All rights reserved. No part of this publication may be reproduced in any form or by any means, electronic or mechanical, including photocopying, recording or any information storage and retrieval system, without permission.

Possible brand names are quoted without any advertising purpose.
Micropole cannot be held responsible for any errors or omissions which may have occurred despite the care and control taken by Micropole.

Follow us!

@MicropoleBeLux
https://belux.micropole.be

Benoit TANCREDI
Partner & Director
Cybersecurity Services

Email | benoit.tancredi@micropole.be
Mobile | +32 (0) 499 93 16 44

Jérôme DOSSOGNE
Cybersecurity Services
Manager

Email | jerome.dossogne@micropole.be
Mobile | +32 (0) 471 87 68 10