


A woman with blonde hair is shown in profile, looking at a large digital screen. The screen displays a complex network diagram with various nodes and lines. The background is a blurred city street at night with warm lights. A large, stylized network diagram with blue lines and nodes is overlaid on the right side of the image. A vertical teal bar is on the left side of the text.

How to operationalize cybersecurity in your organization

SIEMENS

Cybersecurity should top the priority lists for most operators of critical infrastructure networks, including most notable utilities.



A close-up photograph of several hands assembling a puzzle. The puzzle pieces are in various colors: white, yellow, blue, and red. The hands are positioned around the pieces, with some fingers pressing them together. The background is blurred, showing warm, golden light and bokeh effects from out-of-focus lights.

Like any priority,
having a well
thought out plan
that brings all the
pieces of the
puzzle together is
critical.




For utilities,
operationalizing
cybersecurity — putting it
into practice — involves a
concerted effort **to
implement best practices
that strengthen vital
cybersecurity
infrastructures.**

Having a defined
organizational
cybersecurity
strategy that's
enabled by an all-
encompassing,
enterprise-wide
program puts utilities
in the driver's seat.



Utilities with a sound strategy and end-to-end program are in a strong security position, making it possible to address and get ahead of advanced—and continuously evolving—cyberthreats.



A photograph of three business professionals in a meeting. One person is holding a smartphone, another is pointing at a document with a green pen, and a third is looking on. The table is covered with various documents, including a red folder, a blue folder, and a laptop keyboard is visible in the foreground.

Developing a cybersecurity program involves documenting your organizations information security:

- ✓ Policies
- ✓ Procedures
- ✓ Guidelines
- ✓ Standards

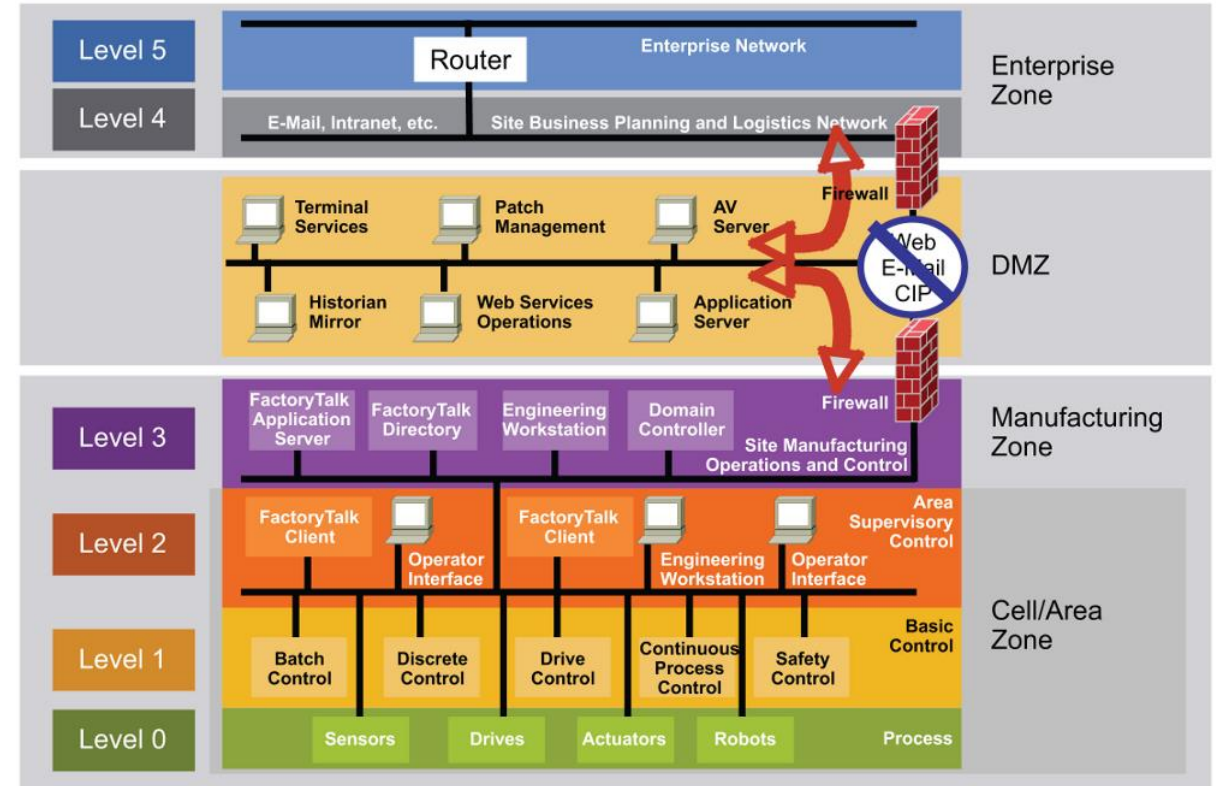
There are 3 different cybersecurity models to consider :

- Purdue Reference Model
- Risk Management Framework(s)
- Cybersecurity Capabilities Model (C2M2)

Option 1

Purdue Reference Model

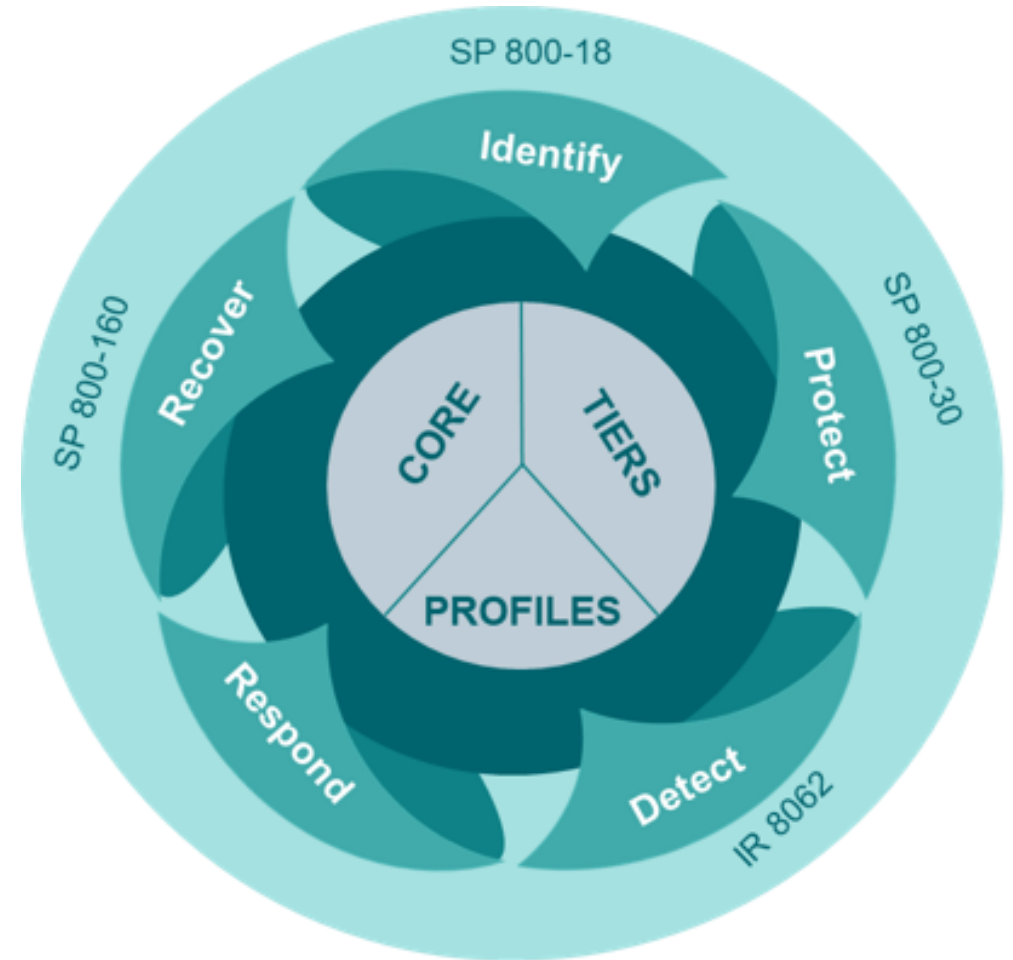
An industry adopted approach that shows the interconnections and interdependencies of all the main components based on hierarchical data flows.



Option 2

Risk Management Framework(s)

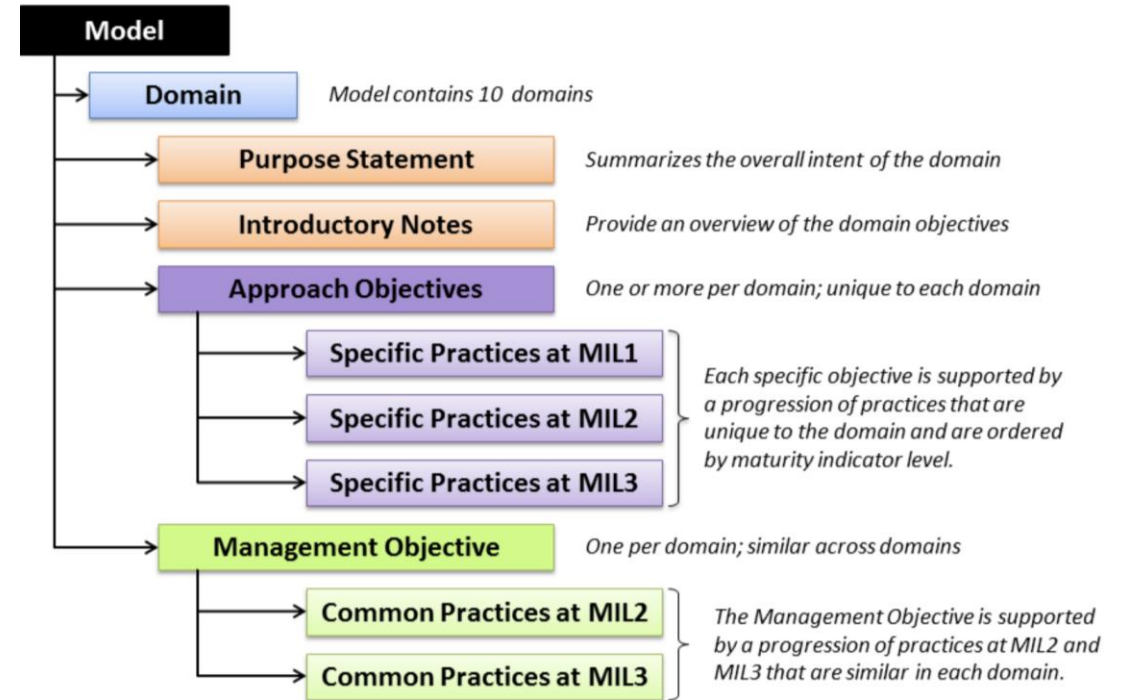
Developed for OT environments, it is the process of identifying potential risks, accessing their impacts and the planning for those impacts.



Option 3

Cybersecurity Capability Maturity Model

Initially developed by the U.S. Department of Energy, it has been adapted for both IT and OT. C2M2 is a voluntary model and assessment tool for building, maintaining and advancing your cybersecurity program.





Strategies are important. Programs are essential. Models are extremely helpful. So is understanding that cybersecurity is an ongoing process.

Always remember these two tips:



Find a standard or framework to operationalize in order to meet your security requirements.

- IEC 62443
- NIST Cybersecurity Framework
- NIST 800-82
- ISO 27001
- ENISA
- CPNI



View your operations from the perspective of an adversary—the bad actors.



While cyber breaches can happen in a flash, utilities must **diligently prepare**, putting in the hard, **thoughtful design work** that can take years.

Siemens understands these challenges.

As a global manufacturer of automation products and digitalization solutions, we hold ourselves accountable to the highest cybersecurity standards and endeavor to lead by example. We have a comprehensive program of technical solutions, services and processes for our customers, combined with certification of external governance organizations and market leading partner solutions. We can assist in your journey to operationalize cybersecurity.

Contact siemensci.us@siemens.com.

SIEMENS



SIEMENS

usa.siemens.com/ruggedcom