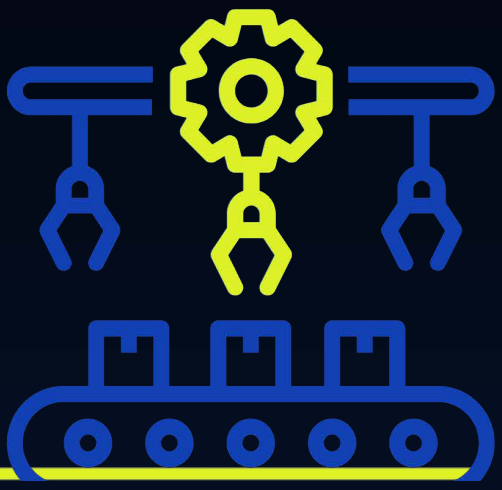
Radiflow

# Ensuring continuity of Risk Management in OT

October 2022



THIS CONTROLLED DOCUMENT IS THE PROPERTY OF RADIFLOW LTD. This document contains proprietary information. Any duplication, reproduction or transmission to unauthorized parties without prior permission of Radiflow is strictly prohibited.
(C) Radiflow LTD. 2022

# 1.Introduction

All companies that run computer systems are not immune to cyberattacks. In recent years, the industry has seen an increase in debilitating attacks on both traditional IT systems and more recently Industrial Automation and Control Systems (Operational Technology [OT]). These attacks have the potential to halt production services across many industries leading to supply chain delays, reputational and revenue impact as well as onward impact to both their customers and business partners.

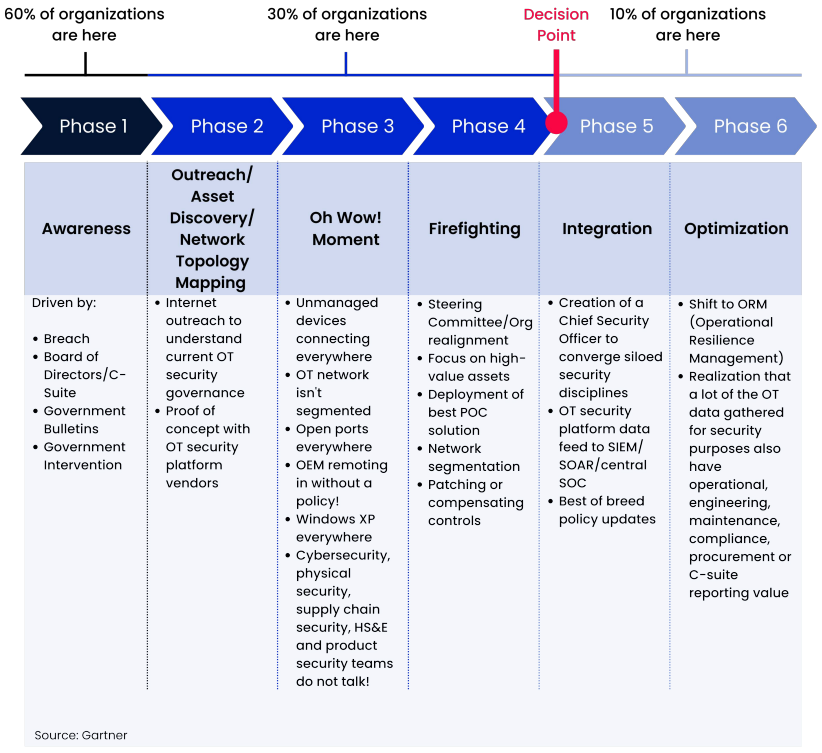
In 2017 the industry was impacted by a widespread notPetya “ransomware” attack that affected many businesses’. One example was an overarching impact across Merck pharmaceutical’s corporate and manufacturing environment which halted production, took months to recover, and resulted in an insurance claim of $1.4Bn.

Responding to cybersecurity risk within an organisation can be triggered through regulations, risk awareness, or potentially through an incident. The journey to Cybersecurity Risk Management maturity within an OT environment is more challenging than in a traditional IT environment which is more mature in embedded security risk management, cyber hygiene (patching), and accountabilities.

Organisations venturing on a journey to reduce and maintain their exposure to OT Cybersecurity Risk will leverage tools, processes, and people to deliver a set of solutions and capabilities that ultimately deliver an acceptable risk posture. [“Securing Pharmaceuticals from OT Cyber Attacks"].

During this journey, organizations will realise the need to implement an OT Security Operating model that enables clear accountabilities and capabilities to sustain risk posture throughout the OT ecosystems life cycles (from purchase to retire).

# 2. The Journey to OT Cybersecurity Risk Management Maturity



The journey within OT often typically gains momentum once a company reaches Phase 3, the “Oh WoW” moment, being able to see what inventory is on the “shop floor”,  knowing the vulnerabilities and risk implications such that action can be taken to remediate risks and then continuously monitor for change.

By no means an easy start in an OT environment where often the sheer numbers of OT systems, such as manufacturing lines, power management systems, building management, warehouse, and so on can dwarf the number of central IT systems and unlike IT are not often well documented in a CMDB. (Configuration Management Database).

Common challenges include:

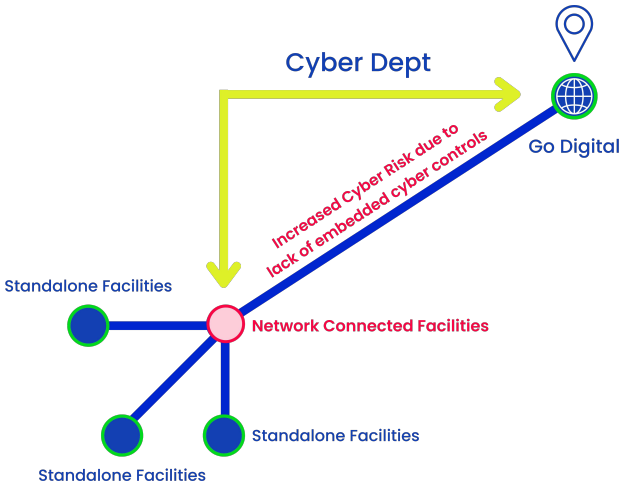
- **Inventory** discovery and risk management capabilities (manual vs tooling).
- **Ageing** OT equipment that is not built for or lends itself to good cyber security hygiene.
- **Language** difference, IT do not speak the same technical language as say an OT Engineer.
- **Accountabilities** for lifecycle management and provisioning of infrastructure and systems.
- **Culture** difference between how an IT organization focuses on patching and lifecycle, vs an engineering organization which typically focuses on Safetity, OEE, Costs of Goods, and keeping old assets running.
- **Production Schedules** reducing the opportunities to patch quickly.

Along this maturity journey, Strategies will need to be jointly agreed with Business, IT, and CISO leaders as a joint venture vs a central remit. As the program of work commences, there will be a stage where it becomes laser clear that an Operating Model needs to be established to ensure the ongoing operation and risk management of OT Security.

# 3. The OT Security Operating Mod

## “Why, What, When, How and Who?”

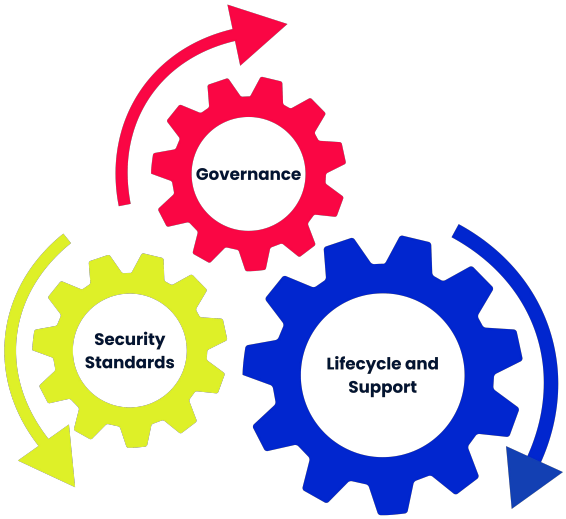
### 3.1 Why is it important?



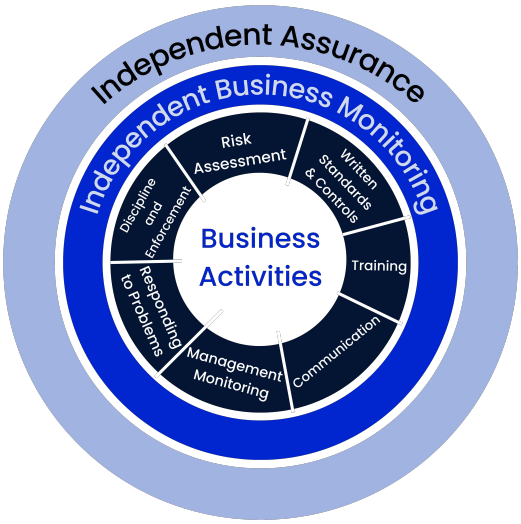

As organisations venture on their digital journey, many facilities and OT equipment, traditionally  standalone from the broader company intranet or the internet are going online to enable the benefits of Digital, Data and Analytics and the forth industrial revolution with IIOT. Whilst this comes with the promise of performance and strong ROI, there is also a “cyber debt” inherited that often is not factored into the “go Digital” ROI, This debt includes the cost of bringing and sustaining an OT environment at the appropriate level of risk from a Cyber Security perspective. In turn this “new” approach to managing the OT environment brings challenges around accountabilities and controls that need to be clarified through a target operating model.

### 3.2 What is it?

It is a model that brings together the target state of how Security, IT and OT practitioners work together to Support, Govern, Standardise and build capability to ensure that the infrastructure, networks and systems in an OT environment are maintained and monitoring at the appropriate level of Cybersecurity risk and capability through the operating lifecycle, from procure to retire.




### 3.3 Governance




A standard governance framework should be adopted and will detail the overarching governance within an organisation. It should be extended to the OT Security TOM to define how and who undertakes governance ensuring the risk posture of the OT Cybersecurity is maintain at a level appropriate to the company's risk tolerance. Independent Assurance would usually be undertaken by either internal or external auditors, whereas Independent Business Monitoring would be effectively self-assessments.

#### 3.3.1 Security Standards

Typically within the IT environment standards will exist that are relevant to Cybersecurity. These will cover topics in the headings below, and will usually be underpinned by one or more standards.

- Infrastructure Security
- Threat and Vulnerability Management
- Identity and Access Management
- Network Security
- Application and Data Security
- Vendor Management (Platforms and Third parties)

IEC 62443, brings a wealth of standards that can pragmatically be adopted and are specifically design of OT (IACS).

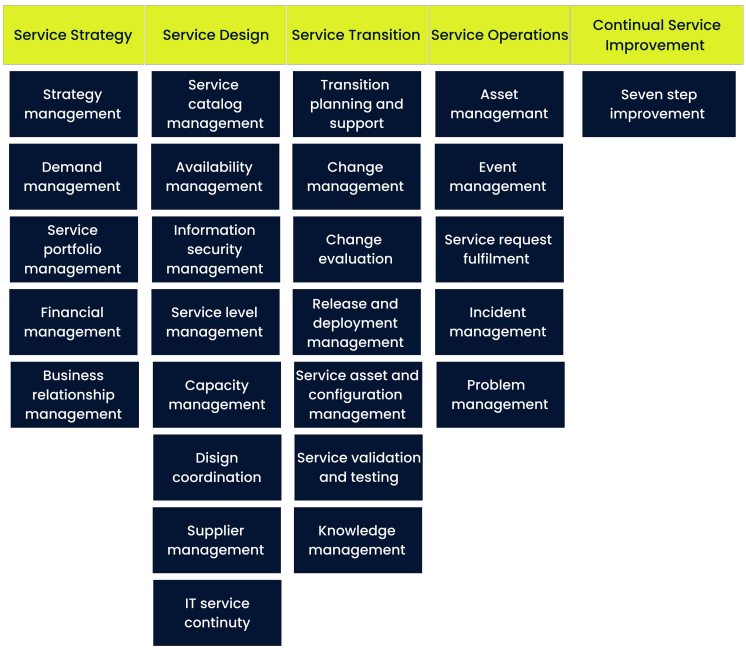
### 3.3.2 Lifecycle and Support

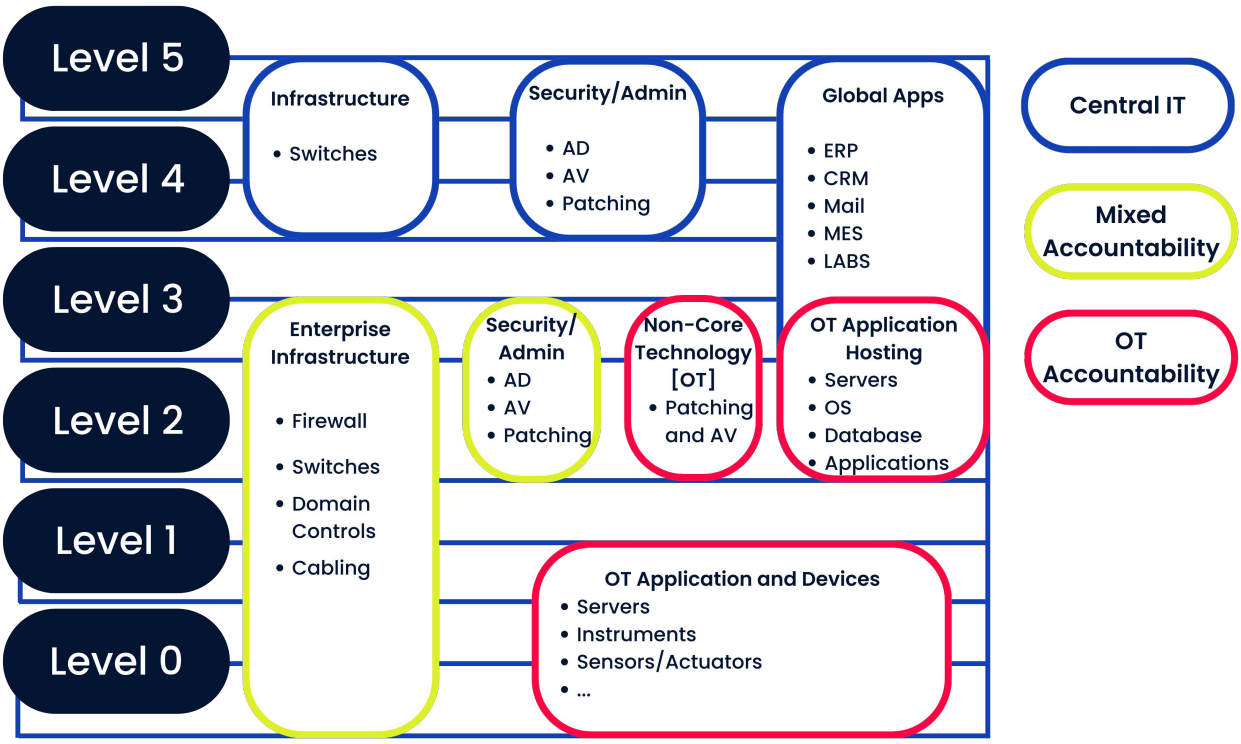
**Support**

Across the layers of the Purdue Model, the accountabilities and responsibilities for support will very. Some may be run by “central IT”, some may be part supported by them and some may be totally run within the OT Operating environment. Accountabilities and responsibilities need to be clarified and consideration to the standard ITIL process framework may help decide what the split is.

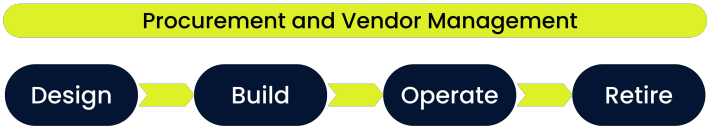
A potential Purdue framework for consideration showing

differences in operating accountabilities is shown below. This may lead to a level of change or at least clarification of accountabilities and support processes.



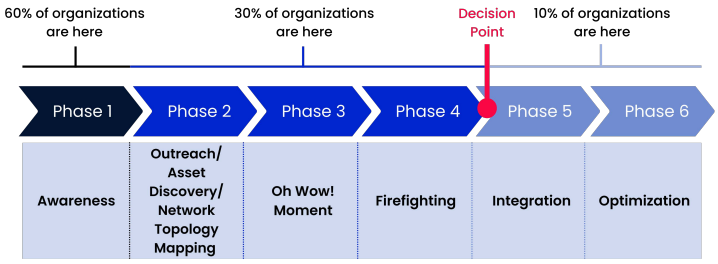




**Lifecycle Management**




In addition to the 2D view of support, a third dimension may need to be applied to agree where accountabilities sit across the lifecycle of an OT asset. As a minimum, it needs to be clear that the OT Security TOM spans the lifecycle and not just the Operate phase.

## 3.4 When to implement it?




Referring back to the earlier diagram showing the journey to maturity, the ideal "When" would be right at the beginning of the transformation journey, as this would help an organisation to start adjusting to change and ways of working. Should an organisation take this approach, it's strongly recommended to have agreed on a joint strategy between the CISO, IT and Business Leaders first and recognised funding to build capability, governance and process.A more agile approach may be preferable, and enable capability and change management to be less dramatic as the organisation grows, learns, and matures together.
As a minimum, an operating model should be agreed upon by the decision point shown between Phase 4 and 5 and an implementation approach agreed. Potential organisation change and skills-building may need to be factored into the adoption as well as the cost impact of adopting OT Security Standards etc.

## 3.5 How to implement it?

At the point of agreeing to commence the operation model as discussed above, serious consideration should be given to implementing security standards that may have not been in place for OT. Organisations may generate or adopt (such as IEC 62443) 20+ standards and consider first adopting those (such as IEC62443) that provide the greatest value in risk reduction. Implementation should be mandated for new OT equipment OR when significant change is made to existing key assets. This will inevitably create some challenges in cost which must need to be factored into the ROI.

Independent Business Monitoring should be a quick win. Training some OT knowledgeable staff and building a periodic assessment schedule within the OT organization. Independent Assurance can be added to the Internal or External auditor's capabilities and carried out periodically.

Support Models ideally should start to be implemented early in the journey, however, that will require some change management or accountabilities and capabilities

Once an operating model is established, and organisation will typically look further and explore how to make OT Security Risk Management routine and leaner. Leveraging tooling that can discover, assess and bring "crown jewel" risk context to the broader OT environment brings a significant reduction in cost and speed over a manual approach.

### 3.6 Who implements it?

A joint venture across OT / IT and Security (CISO) will be required. A project lead should be appointed with all parties participating at a joint steering committee to measure progress and resolved issues.

## 4. Radiflow's solutions for optimising Security Risk Management Operating Models

Leveraging technology for discovery and risk management of OT-connected systems and devices can both accelerate an organisations understanding of its risk posture and provide ongoing and near real-time visibility to a changing internal and external threat landscape. Radiflow's products bring industry excellence in the discovery and risk management of OT at the enterprise level with additional industry-leading value from enterprise risk visibility, laser-focused reporting, and planning by critical assets. These products will enable a CISO to quantify and prioritise risk and impact in ways that business owners will understand and jointly support funding proposals.

Radiflow's OT-security suite has been successfully implemented in a number of major organisations worldwide. Radiflow's multi-prong solution provides anomaly detection and threat monitoring within an OT environment (manufacturing, utilities, transportation, power etc) to ensure the detection of breach attempts originating from the IT network. The Radiflow solution further improves network oversight by providing full visibility (via network "maps") into the OT network, including all device properties, vulnerabilities, communication protocols, and possible intra-network attack vectors.

tack on each zone/business unit or critical asset) and subsequently, the mitigation measures best suited to reducing the most risk and thus increasing the ROI of the entire cybersecurity operation.

Radiflow's risk assessment process involves analysing thousands of network data points and asset properties, threat intelligence, and impact calculation to provide various KPIs and full reports for the network's risk state:

- Infrastructure Security
- Network and asset properties: using non-intrusive self-learning of the OT network, Radiflow creates a complete digital image of the network with all networks, communications, and assets properties and vulnerabilities. The digital image serves as the baseline activity model for assessing risk and OT cybersecurity planning.
- Threat intelligence: newly-detected threats and threat players' capabilities are analysed and published by a number of dedicated agencies (e.g. MITRE ATT&CK) as well as by others, including Radiflow's own research.
- Zone impact & criticality, risk tolerance, and other considerations: assets and business processes are grouped into zones with different levels of criticality and security needs.


Radiflow's CIARA OT Risk Assessment & Management Platform analysing thousands of data points for network and asset properties, threat intelligence, and impact calculation, toward providing various KPIs and full reports for the network's risk state.

All asset, network, threat, and SuC owner-provided data points are used to run numerous non-intrusive breach and attack simulations

The simulations determine the most impactful threats to the network and subsequently, the most effective mitigation controls that deliver the most risk reduction per dollar spent.

The results of Radiflow's risk assessment are provided in the form of various high-level and detailed reports used for budgeting, auditing, and follow-up, as well as a detailed mitigation plan listing the most effective (high-ROI) mitigation measures, accounting for the user's budget and risk management preferences.

## 5. Conclusion

The journey to mature Cybersecurity risk management in an OT environment takes investment in technology, people, and process. With a significant investment getting past the "oh wow" moment and implementing initial risk remediation steps, it is essential to recognise the need to embed and sustain a risk management approach and investment with potential organisation changes being required to sustain the investment and security posture.

Many organisations build a hybrid of SOC / SIEM and CMDB integration, along with a level of manual process, often built into the Security team or embedded within the OT teams to keep on top of a changing threat landscape.

The next step in a maturity journey is how to make it lean, or make it routine.  A combination of a clear OT Security Operating model and leveraging technology will reduce the cost of sustaining an organisations risk posture as well as bringing a greater level of agility and speed to detect, identify and respond to threats and vulnerabilities.

### About Radiflow

Radiflow develops unique OT cybersecurity tools to protect and ensure organizations' digital resilience. The company closely collaborates with Managed Security Service Providers to oversee the discovery and management of all relevant data security points. Founded in 2009, Radiflow has offices and partners in Europe, USA and APAC. Its field-proven solutions are installed at over 7000 sites around the globe.

(C) 2022 Radiflow LTD. All Rights Reserved. Radiflow reserves the right to change product specifications without prior notice.