CYBERSECURITY SERVICES REGULATION OFFICE

# BUYER'S GUIDE FOR MANAGED SECURITY OPERATIONS CENTRE

## "When an alarm bell sounds, it might be too late"

## 1. What is a Managed Security Operations Centre ("MSOC")?

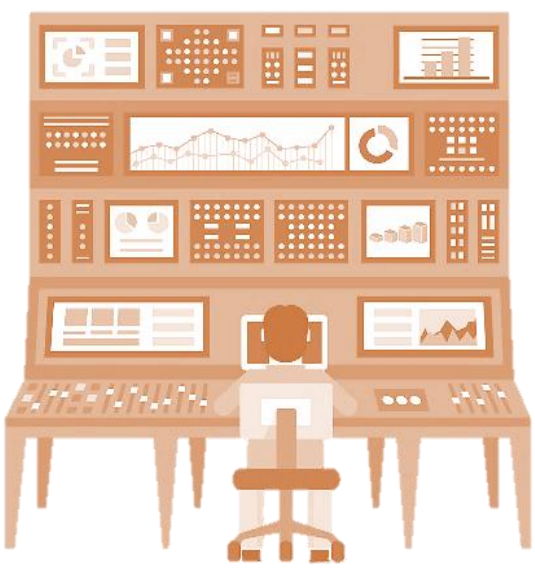
A MSOC provides an around-the-clock cost-effective solution to **continuously monitor, analyse your organisation's security posture** for protection against both external and internal/insider cybersecurity threats and **respond promptly to cybersecurity incidents**.

An effective MSOC is **fundamentally built on good cybersecurity concept-of-operations** by adopting and integrating good technological solutions and tools, sound processes and developing a team of security analysts and engineers who serve as the first responders to cybersecurity threats and incidents to prevent or minimise damage to your organisation's cybersecurity posture as a result of a cyber-attack in a timely manner.

## 2. Why do I need a MSOC?

Cyber-attacks are rapidly evolving and adversaries are always on the hunt to wreak havoc on your organisation's cyber defence posture for monetary gain, political objectives or for fame.

With the proliferation of digital technologies and greater reliance on the Internet for business transactions, it has become increasingly important to engage a good MSOC that can help to **actively monitor and promptly respond to cybersecurity threats and incidents** so as to avoid or minimise damage to your organisation's cybersecurity posture.



## 3. What are the available options?

**Organisations may choose to implement their own dedicated Security Operations Centre.** This would include procuring and integrating technological solutions and tools; and developing the processes for a team of security analysts and engineers to actively and effectively monitor and respond to evolving cybersecurity threats and incidents to strengthen your organisation's cybersecurity posture. Alternatively, **outsourcing to a licensed MSOC could be a cost-effective solution** to leverage on the industry expertise and tools without significant upfront investment in technologies and manpower, which is particularly challenging in the manpower scarce industry.

Disclaimer: This guide is produced by the Cybersecurity Services Regulation Office as an introductory guide for buyers of MSOC services. Buyers are advised to do their due diligence when selecting a licensed MSOC service provider and to consult relevant references to ensure that their requirements are met.

# "Okay, I do need to engage a MSOC, what's the next step?"

## START by knowing your organisation's cybersecurity posture and risk exposure

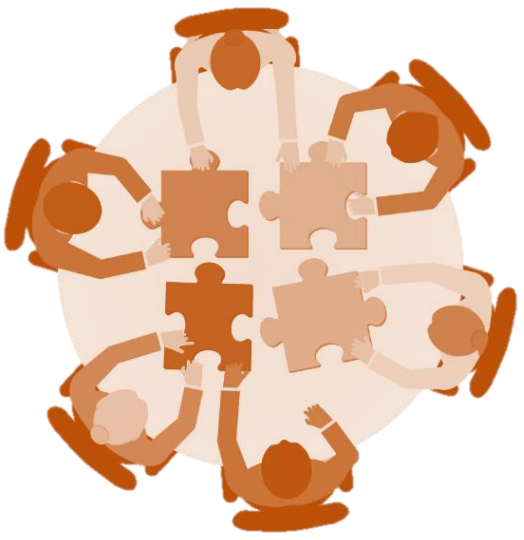
Conduct a risk assessment to identify what you need to protect and the external and internal/insider risks and threats to your organisation's IT infrastructure and digital assets.

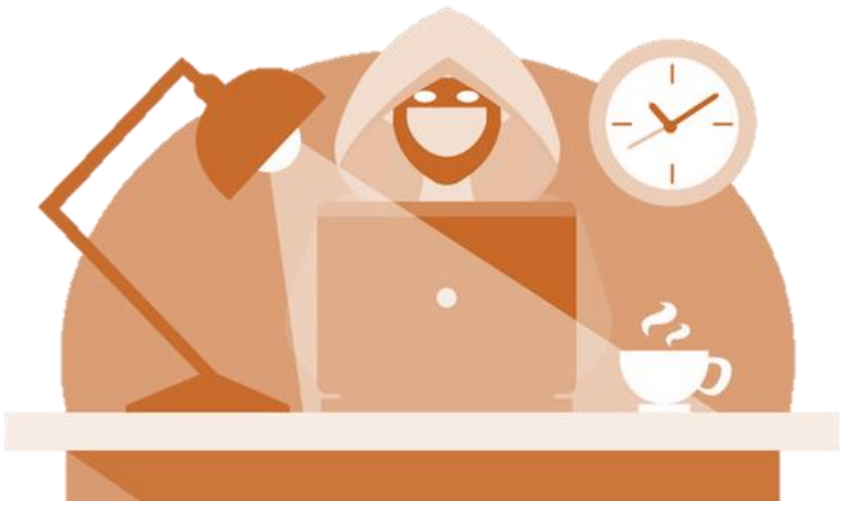
## DEFINE requirements for the MSOC

Determine the engagement scope, deliverables, budget, and timeline.

## EVALUATE the available options

Based on the information gathered, assess the available options and form a project evaluation team that is familiar with your organisation's cybersecurity posture and requirements.





## CONSULT a licensed MSOC service provider for assistance

MSOC service provider would take a holistic view of the organisation's internal and external environments and provide you with guidance on the scope your organisation requires at a reasonable cost. Obtain proposals from multiple licensed MSOC service providers before deciding which best suits your requirements.

Disclaimer: This guide is produced by the Cybersecurity Services Regulation Office as an introductory guide for buyers of MSOC services. Buyers are advised to do their due diligence when selecting a licensed MSOC service provider and to consult relevant references to ensure that their requirements are met.

# 4. How to select a licensed MSOC service provider?


Review the experiences, credentials and qualifications of the licensed MSOC service provider and the individual support personnel

- Check whether the MSOC service provider is licensed.
  ***Tips***: *CSRO website (QR code on right) provides a list of licensed MSOC service provider.*
- Understand how does the licensed MSOC service provider keep up with the rapidly evolving MSOC technologies and skillsets.
  ***Tips***: *Consider factors such as timely acquisition of technological solutions, tools and staff trainings.*
- Understand the current and past clients/projects of the licensed MSOC service provider. Request them to provide references from their clients with similar profiles as your organisation.
  ***Tips***: *Consider size of organisation, business nature, challenges and resolution provided.*
- Verify the individual support personnel's experiences, qualifications and professional certifications.
  ***Tips***: *Some relevant certifications include ISO/IEC 27001 Information Security Management, System and Organisation Controls 2, GIAC Continuous Monitoring Certification, GIAC Information Security Professional, CREST Threat Intelligence Analyst and CREST Practitioner Security Analyst.*

Assess the plan proposed by the licensed MSOC service provider

- Ability of the licensed MSOC service provider to develop, integrate and interoperate their processes with your organisation's existing processes and IT systems and network infrastructure.
- Clearly defined critical success factors and key performance/mission indicators that are quantifiable, measurable, organized hierarchically and tracked regularly at appropriate reporting levels.

Understand your licensed MSOC service provider's liability and insurance coverage as you are entrusting the protection of your organisation's assets and sensitive data such as IT infrastructure, operational blueprints and digital assets to them and there is a risk that things may go the wrong way e.g. loss of sensitive or proprietary data. Contract with the licensed MSOC service provider should be referred to a legal team (or equivalent) to review the terms of business, details of the contract and schedule of work from legal standpoint.


# 5. How to proceed with the chosen licensed MSOC service provider?

The following is a **typical workflow** when engaging a licensed MSOC service provider:

- Start with planning, preparation and working together with the licensed MSOC service provider to define an approach that incorporates your organisation's goals, risk appetite and requirements.
- Next, the licensed MSOC service provider will gather extensive information on your organisation's infrastructure, systems and identify the exposure to external and internal/insider cybersecurity threats.

- This is followed by implementing new processes and integration with existing processes to monitor and respond to cybersecurity threats and incidents.
- Lastly, obtain regular reports from the licensed MSOC service provider which include high-level management style reporting and technical details on the organisation's cybersecurity posture and exposure to the cyber threat landscape.

Disclaimer: This guide is produced by the Cybersecurity Services Regulation Office as an introductory guide for buyers of MSOC services. Buyers are advised to do their due diligence when selecting a licensed MSOC service provider and to consult relevant references to ensure that their requirements are met.