Portfolio Rationalisation

Built for Microsoft Azure
Active Directory

pwc | Microsoft

The cybersecurity portfolio challenges organisations face today

With a consistent flow of new, “best of breed” solutions and an ever-changing set of requirements, managing an organisation's cybersecurity tool portfolio has become harder than ever. The diagram below highlights some of the challenges cybersecurity groups face today with their tools:

Underleveraged Tools

Tools that are are already purchased, but are not being used to the full extent of their capabilities

Redundant Tools

Multiple tools within the organisation that have overlapping capabilities

Incompatible Tools

Tools from varying providers that may be the best of breed, but are difficult to integrate and create a compatible, integrated cybersecurity portfolio

Varied Experiences

Inconsistent user experiences across the enterprise resulting in reduced efficiency and confusion

Overspending

Overpaying for cybersecurity capabilities by purchasing best of breed solutions in each security domain as opposed to efficiently enabling compatible, bundled tool suites that have already been purchased

Low Portfolio Visibility

Lack of understanding of what tools are actually owned by the organisation what capabilities those tools support

Cybersecurity Gaps

Gaps in the cybersecurity program that are not currently addressed by any of the tools in the cybersecurity portfolio

Our service offering – Portfolio Rationalisation

Utilising a collaborative, workshop based approach, PwC's Portfolio Rationalisation holistically assess your organisation's security capabilities across the enterprise, identify areas of improvement, and facilitate the adoption of Microsoft 365 cybersecurity technologies to Utilise, Rationalise, and Optimise your cybersecurity portfolio.

1 Utilise
Use tools' full potential

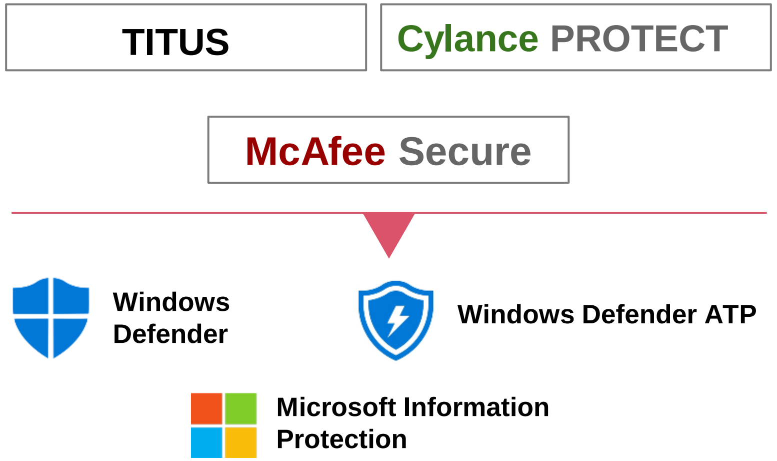
- ✓ Exchange
- ✓ SharePoint
- ⊗ Azure Active Directory
- ⊗ Windows Defender
- ⊗ Windows Defender ATP
- ⊗ Microsoft Information Protection

LEGEND
- ✓ Owned and Used
- ⊗ Owned but not utilised

Underleveraged Tools

We can help leverage the full potential of tools and optimize your security spend by identifying solutions within your current product stack which are under utilised. For instance, identifying cybersecurity technologies within the Microsoft E3 and E5 offerings which could be used to protect your environment

2 Rationalise
Security tool landscape


TITUS

Cylance PROTECT

McAfee Secure

Windows Defender

Windows Defender ATP

Microsoft Information Protection

Redundant Capabilities

Rationalising your security solutions can not only reduce security spend by reducing redundant capabilities, but also increase integration between your technologies

3 Optimise
Address gaps in cybersecurity capabilities

10 Cybersecurity Domains:

Asset & Systems Mgmt.	Vulnerability Mgmt.
Gov., Risk & Compliance	Encryption & Key Mgmt.
Identity & Access Mgmt.	Network Security
Data Protection	Logging & Monitoring
Secure Cloud	Incident Response & Forensics

Gaps in Cybersecurity Capabilities

Gaps within an organisation's cybersecurity capabilities can be easily identified and addressed by assessing your capabilities across the 10 Cybersecurity domains Furthermore the technology capability that may be needed to address the gap may exist in your Technology stack today!

Key phases of the Portfolio Rationalization process

The work for portfolio rationalization process is spread across three phases: Before the Session, the Portfolio Rationalization Session itself, and the activities After the Session:

1 Before the Session

Provide a questionnaire, glossary of key terms, and pre-session communication to **understand client's focus areas and current state of tools** environment

Questionnaire (client responds)

- Strategic Direction
- Core Business Functions
- Cybersecurity Tools Landscape & Capabilities
- Standards, Regulations & Industry Best Practices
- Cost of Ownership

Glossary of Key Terms
(from Microsoft & PwC)

2 Portfolio Rationalisation Session

Identify overlaps between client's existing tools and Microsoft tech. and understand how we can help **address the gaps** and help **rationalise the capabilities**

10 Cybersecurity Domains:

Asset & Systems Mgmt.	**Vulnerability Mgmt.**
Gov., Risk & Compliance	**Encryption & Key Mgmt.**
Identity & Access Mgmt.	**Network Security**
Data Protection	**Logging & Monitoring**
Secure Cloud	**Incident Response & Forensics**

3 After the Session

Develop documentation to recap key pain-points and opportunities. Assist with **additional discussions, workshops and projects** (as necessary)

Provide Action Plan & Roadmap
outlining key pain-points and opportunities

And

Assist with additional projects, workshops, and/or discussions
to bring the action plans to life, and best fit your cybersecurity roadmap

Phase I – Before the session

Prepping for the session is paramount as it ensures that the session itself with be productive. The activities that occur before the portfolio rationalisation session are summarised below:

Determine which of the 10 domains you would want to focus

- Provide an introduction and overview of the 10 Cybersecurity domains
- You identify key pain points or focus areas
- Understand key next steps
- PwC will also provide a Glossary of Key Terms

Provide the questionnaire and collect client's responses

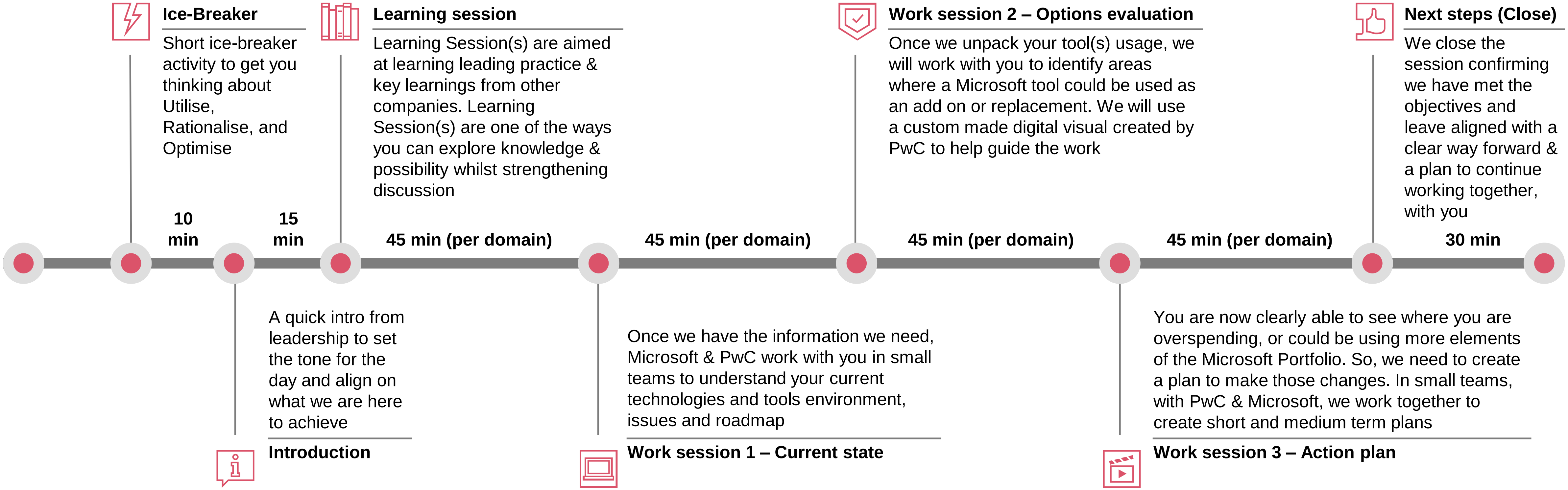
- We will send pre-session questionnaire to you with a user guide & examples
- You respond with filled questionnaire
- We will synthesiae your responses to find the best way to meet your needs

Pre-Session Prep. Sessions with the Client, PwC & Microsoft teams

- Provide a short description of each of activity and the roles to be filled
- Confirm who will be attending the session from their side in each area
- Review session schedule & activities
- Finalise RACI and obtain confirmation
- Finalise session-supporting technology details

Phase II – The portfolio rationalisation session

The session itself is where PwC, Microsoft, and the organisation together to make sense of the organisation's cybersecurity portfolio, identify "hot spots" or key rationalisation areas, and develop the core of the go-forward action plan. The session activities are summarised below:



Ice-Breaker

Short ice-breaker activity to get you thinking about Utilise, Rationalise, and Optimise

10 min

Introduction

A quick intro from leadership to set the tone for the day and align on what we are here to achieve

15 min

Learning session

Learning Session(s) are aimed at learning leading practice & key learnings from other companies. Learning Session(s) are one of the ways you can explore knowledge & possibility whilst strengthening discussion

45 min (per domain)

Work session 1 – Current state

Once we have the information we need, Microsoft & PwC work with you in small teams to understand your current technologies and tools environment, issues and roadmap

45 min (per domain)

Work session 2 – Options evaluation

Once we unpack your tool(s) usage, we will work with you to identify areas where a Microsoft tool could be used as an add on or replacement. We will use a custom made digital visual created by PwC to help guide the work

45 min (per domain)

Work session 3 – Action plan

You are now clearly able to see where you are overspending, or could be using more elements of the Microsoft Portfolio. So, we need to create a plan to make those changes. In small teams, with PwC & Microsoft, we work together to create short and medium term plans

45 min (per domain)

Next steps (Close)

We close the session confirming we have met the objectives and leave aligned with a clear way forward & a plan to continue working together, with you

30 min

10-15 Participants per Session	One (1) Day Session (with pre-session communications)	Any Location (also available virtually)

Phase III – After the session

With an understanding of the organisation’s current technology portfolio as well as key areas to efficiently help optimise the organisation’s security capabilities, PwC delivers a formal deliverable package consisting of pre-session materials, the session highlights, and a formal action plan:

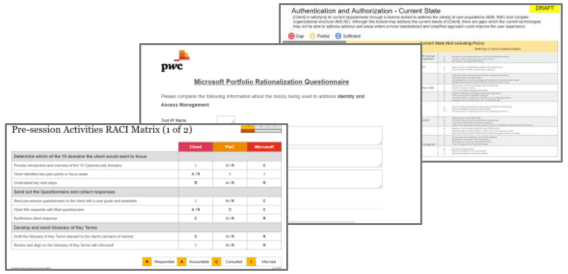
Key outputs

Pre-session –
- Completed Portfolio Questionnaire
- RACI Document
- Glossary of Key Terms

Portfolio rationalisation session –
- Current State Report
- Rationalisation Options

After session –
- Action Plan and Roadmap

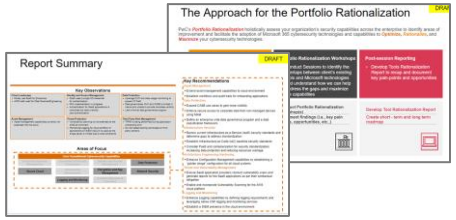
Sample deliverables


Authentication and Authorization - Current State

DRAFT

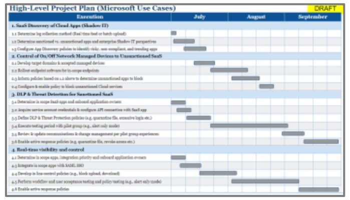
Microsoft Portfolio Rationalization Questionnaire

Pre-session Activities RACI Matrix (1 of 2)


The Approach for the Portfolio Rationalization

Report Summary

DRAFT


High-Level Project Plan (Microsoft Use Cases)

DRAFT

Our commitment

We will work with you to bring the action plans to life through additional workshops, projects, or discussions to best fit your cybersecurity roadmap

Learn more

Contact us to learn more about how you can transform your cybersecurity operations

Haitham Al-Jowhari
Partner
Haitham.Al-Jowhari@pwc.com
+971 56676 1146

James Toulman
Director, Cloud Services
James.Toulman@pwc.com
+971 56227 1811

Thank you

pwc.com/me