CISO AS A SERVICE

Protect. Govern. Assure.

Executive cybersecurity leadership connecting risk exposure, accountability, resilience and investment.

Govern cybersecurity as a business risk, not as a technical checklist.

Cybersecurity has become critical to business performance, operational continuity, reputation and regulatory compliance. As threats evolve and expectations from regulators, clients and insurers increase, organisations need experienced leadership to support informed decisions.

CISO as a Service provides flexible, senior-led cybersecurity leadership aligned with your organisation's business risks and priorities.

WHY IT MATTERS

THE QUESTION EVERY LEADERSHIP SHOULD ASK

EXPOSURE

Do we understand our most significant cyber risks?

OWNERSHIP

Are cyber responsibilities and decision rights clearly defined?

RESILIENCE

Are we prepared to respond to and recover from disruption?

INVESTMENT

Are security investments aligned with business risk and priorities?

EXPOSURE ▶ OWNERSHIP ▶ RESILIENCE ▶ INVESTMENT

CLEARER CYBER RISK DECISIONS. STRONGER BUSINESS RESILIENCE.

RSM Switzerland SA is a member of the RSM network and trades as RSM. RSM is the trading name used by the members of the RSM network. Each member of the RSM network is an independent assurance, tax and consulting firm each of which practices in its own right. The RSM network is not itself a separate legal entity of any description in any jurisdiction.

Each member of the RSM network is an independent assurance, tax and consulting firm each of which practices in its own right. The RSM network is not itself a separate legal entity of any description in any jurisdiction. The RSM network is administered by RSM International Limited, a company registered in England and Wales (company number 4040598) whose registered office is at 200 Aldersgate Street, London, EC1A 4HD, United Kingdom. The brand and trademark RSM and other intellectual property rights used by members of the Network are owned by RSM International Association, an association governed by article 60 et seq of the Civil Code of Switzerland whose seat is in Zug.

WHAT YOU RECEIVE

From cyber exposure to accountable action.

CISO as a Service provides structured, senior-led cybersecurity leadership to help management understand exposure, establish ownership, prioritise investment and strengthen resilience.

SIX KEY DELIVERABLES

01 | BUSINESS-ORIENTED CYBER RISK VIEW

A consolidated view of the cyber risks requiring management and leadership attention.

02 | DEFINED GOVERNANCE & OWNERSHIP

Clear cyber risk responsibilities, decision rights and accountability.

03 | PRIORITISED SECURITY ROADMAP

A structured roadmap focused on the most important risks, dependencies and improvement priorities.

04 | BOARD-LEVEL DASHBOARD

Clear reporting to support management and Board-level oversight of cybersecurity.

05 | BUDGET & INVESTMENT PRIORITIES

Greater clarity over cybersecurity investment needs and priorities.

06 | CONTINUOUS IMPROVEMENT PROGRAMME

A structured approach to strengthening cybersecurity governance and maturity over time.

HOW IT WORKS

A pragmatic approach to move from analysis to action.

FRAME

Clarify the business context, cybersecurity concerns, decisions and constraints.

ASSESS

Establish cyber exposure, priorities, dependencies and leadership needs.

DECIDE

Agree priorities, governance, ownership and risk responses.

ACT

Mobilise the cybersecurity roadmap and agreed next steps.

CYBERSECURITY AS A BUSINESS RISK

Connecting cyber exposure with ownership, resilience and investment decisions.

CISO as a Service provides structured, senior-led cybersecurity leadership to help management understand exposure, establish ownership, prioritise investment and strengthen resilience.

Exposure

Understand material cyber risks.

What could have a material impact on the business?

OWNERSHIP

Clarify accountability.

Who owns the risk, decisions and actions?



RESILIENCE

Strengthen preparedness.

Can the organisation respond, recover and continue operating?

INVESTMENT

Prioritise resources.

Where should leadership invest, strengthen controls or accept risk?

Effective cybersecurity governance connects risk exposure with clear ownership, resilient operations and informed investment decisions.

WHY RSM SWITZERLAND

Independent perspective. Senior-led advice. Business-first decisions.

RSM Switzerland combines business understanding with technology, governance and risk expertise to provide an independent perspective on the issues that matter most. Where deeper specialist capabilities are required, relevant expertise can be mobilised across cybersecurity, data and AI, transformation, resilience, regulatory compliance and the wider RSM network.

RSM at a Glance

Swiss expertise. Global capabilities.

Local expertise

With offices in Geneva, Lausanne, Sion and Zurich, we support organisations across Switzerland through close client relationships and in-depth market knowledge.

National coverage

Your dedicated Swiss contact coordinates the right specialists and services, ensuring a seamless and efficient experience.

Connected globally

As part of the RSM network, we provide access to international expertise, specialist insight and cross-border capabilities whenever required.





LET'S DISCUSS YOUR TECHNOLOGY PRIORITIES

Start with a 30-minute executive to clarify your cyber exposure, ownership, resilience and investment priorities.

Pierre Messus

CIO – Head of IT & Risk Advisory

pierre.messus@rsmch.ch

DL: +41 22 888 50 50

Contact Pierre