

ASSESSMENT AND COMPLIANCE SERVICES

How Hitachi Systems Security can help you comply with the information risk management guidelines of the Quebec's Autorité des Marchés Financiers

Hitachi Systems Security offers integrated cybersecurity services to help you meet challenges of today and tomorrow.

**WE ARE AN
EXTENSION OF
YOUR TEAM**



Managed Security



Professional Services



5 5 security centers worldwide

50+ Countries

1999 Founded in 1999

We are at the service of companies in several sectors

Finance



Telecommunications



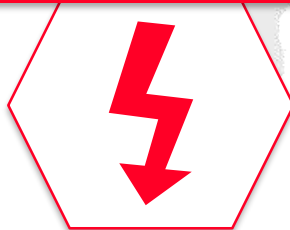
Health



Government



Energy



Retail



24/7 MANAGED IT SECURITY SERVICES

24x7 REAL-TIME THREAT MONITORING | MONTHLY EXECUTIVE REPORTS | ACCESS TO THE ARKANGEL CONSOLE

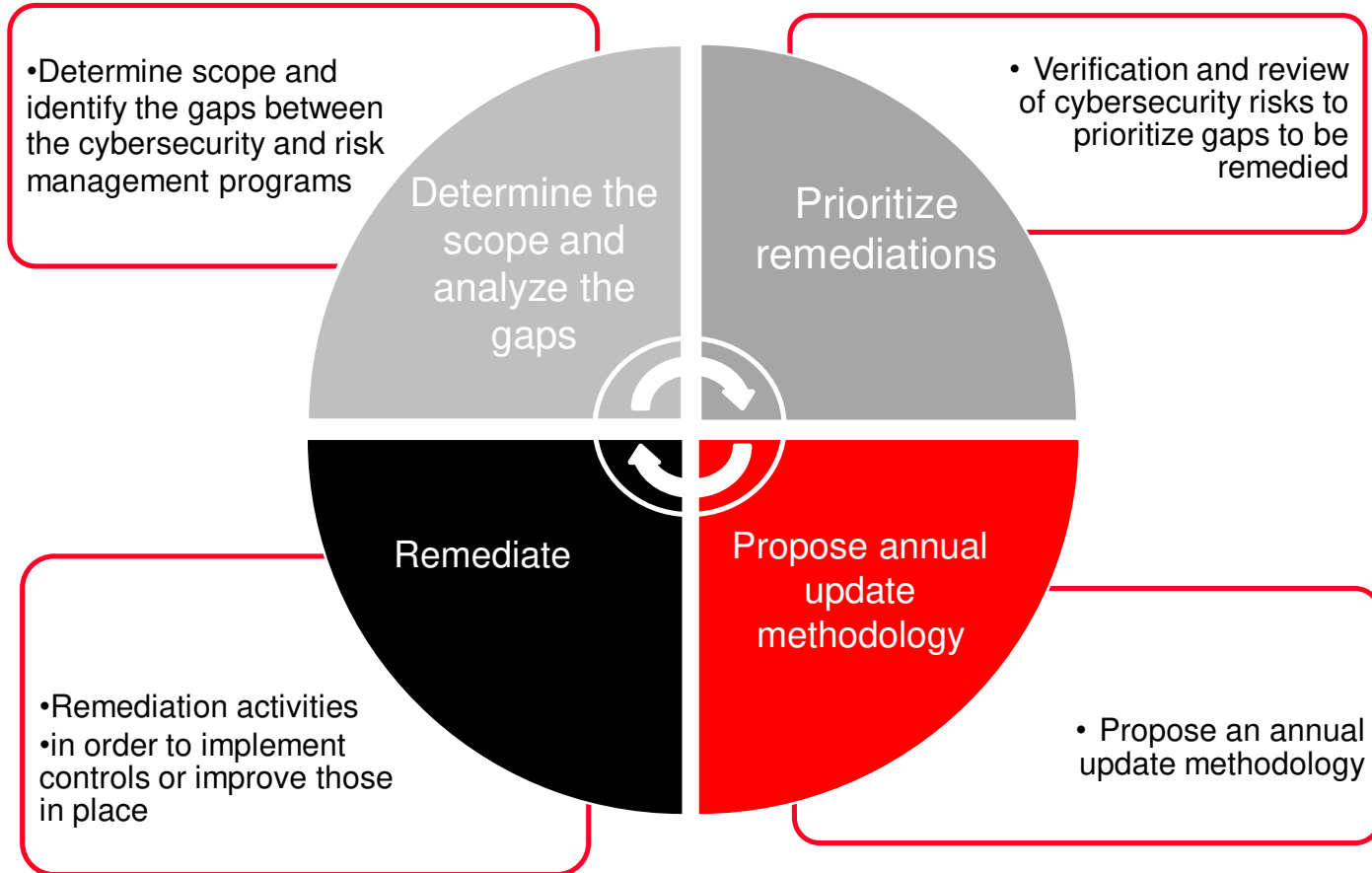
- ✓ Guaranteed incident reporting within 2 hours
- ✓ Dedicated Information Security Specialist
- ✓ Cloud security monitoring
- ✓ Event Correlation and real-time log analysis
- ✓ Integration with existing technologies
- ✓ Monitoring and follow up of security events
- ✓ Threat Intelligence
- ✓ Vulnerability management
- ✓ Continuous detection of abnormal activities on network infras


PROFESSIONAL SERVICES

ASSESS YOUR SECURITY POSTURE | ALIGN YOUR SECURITY STRATEGY WITH YOUR BUSINESS OBJECTIVES | IDENTIFY YOUR VULNERABILITIES

- ✓ Cyber security posture assessment
- ✓ Penetration tests, phishing, code review, WIFI tests
- ✓ Inventory and classification of assets
- ✓ GDPR compliance, Privacy, Confidentiality policies
- ✓ Compliance to ISO 27001
- ✓ DPO and CISO as a Service
- ✓ Privacy by Design support
- ✓ Cloud security (before, during and after deployment)
- ✓ DR, BCP

How Hitachi Systems Security can support your compliance program towards the AMF requirements





Know your compliance posture with AMF requirements

Understanding where you are, where you need to go and what to do to get there

Targeted spending to strengthen your compliance and risk management posture

Help with Law project 64 compliance regarding protection of personal information

Avoid fines and reputation damage

Activities and deliverables

1. Gap analysis and priority improvement plan
2. Assessment of the maturity of cybersecurity controls, based on a combination of recognized industry standards **and** according to the compliance requirements of the AMF:
 - ISO27001, NIST SP 800-37 + NIST SP 800-39 (cyber security risk management) and COBIT 5
3. Remediation to reduce or eliminate gaps
4. Annual update process and document retention
5. Compliance report that can be delivered to the AMF, if necessary



HITACHI
Inspire the Next 