
quillon
STRENGTH IN SERVICE

CRITICAL INSIGHT. TRUSTED CARE.

- SECURITY RISK MANAGEMENT
- BUSINESS INTELLIGENCE
- CYBER RISK MANAGEMENT
- PROTECTIVE SERVICES

LET'S SECURE YOUR ORGANIZATION

With Quillon as your security partner, you get measurable risk reduction against all types of vulnerability. We view security through a lens of integrity and actively engage with the people who are under our trusted care.

Whether protecting properties, bank accounts or reputations, our team powers your success by protecting your most valuable assets. You get the safest and strongest possible resolutions to any threatening situation while maximizing your security investment.

STRENGTH IN SERVICE

At Quillon, we design customized risk management solutions and security services that protect you against the exact threats you face. And we do it using a tailored, hands-on approach that prioritizes the service you receive.

Led by a veteran and international security leader, our team is committed to meeting the highest global standards for tactical strategy, advanced technology and critical insight.

HOW WE CAN HELP

When your organization needs assistance with risk management, business intelligence services, cyber risk management, non-policing services, or boots-on-the-ground protection, Quillon delivers peace of mind. We bring unparalleled service and decades of top-tier international experience in public and private sectors and non-governmental/not-for-profit organizations.

FIT-FOR-PURPOSE SECURITY SOLUTIONS

SECURITY RISK MANAGEMENT

Our Security Risk Management services include embedded or virtual security manager, framework and policy development, risk assessments, consulting, continuity, and crisis management, as well as security training.

When facing any threatening situation, you can count on the industry's most accomplished threat and risk management professionals to help you reach the safest possible resolution. You'll gain an understanding of the level of threat and risk you face along with an assessment of the likelihood of the threat.

Everything we do is rooted in international best practices, and our approach is carefully measured against other intelligence and protective efforts to ensure safety and security for you, your family , corporation and reputation.

EMBEDDED OR VIRTUAL SECURITY MANAGER

Providing security expertise without the cost and headcount of a full-time security manager.

Quillon can help you navigate the challenging organizational problems you face. We can provide your organization with a seasoned security practitioner with exacting standards and an understanding of complex international organizational challenges.

Ask yourself the following questions:

- Does your organization need occasional expert security advice, mid- to senior-level guidance but don't want the additional headcount and cost of a security director?
- Are you rethinking your company's security structure and unsure on the best route to take?
- As a cost saving measure and reduced headcount, are you considering an outsourced solution but don't want to compromise your company's security posture?
- Do you have a security team in house but aren't getting value for money? Is a review or mentoring program needed to support your current security team?
- Has your organization grown faster than you've been able to keep up organizationally and need additional expert security personnel?

If the answer is "yes", Quillon can help.

Whether you need part-time, full-time, long-term, short-term, in person or virtual assistance, we have a fit-for-purpose solution to align with your organization's needs, anywhere in the world.

SECURITY STRATEGY, POLICY, PROCEDURE DEVELOPMENT AND IMPLEMENTATION

Evaluate your organization's current policies or put new ones in place to meet your needs at home or in other countries.

Given the complexity of your organization, it can be overwhelming to start putting effective security frameworks and programs in place. We can help you create security policies and procedures that work together to close the gaps that might otherwise expose your organization to greater risks. And we'll ensure everything is aligned to your strategic plan.

We'll work with you to consider policies and procedures that cover risks like workplace violence, bomb threats, active shooters or natural disasters. Perhaps you're considering executive protection for travel to high-risk areas? How do you know if current procedures will be sufficient or effective?

We can work with you to develop security policies tailored to the exact risks you face—all within the framework of laws and regulations of each country you operate in. Depending on your needs, we can assist with comprehensive security programs or individual components, such as access control, pre-employment background checks, workplace violence prevention or executive protection.

SECURITY RISK MANAGEMENT

SECURITY RISK ASSESSMENTS

Mitigate risks associated with terrorism, workplace violence, corporate espionage, theft and more.

Are your organization, staff and infrastructure prepared for physical security risks? Our security professionals can help you determine the likelihood of any particular threat, prioritize action plans, recommend appropriate security measures and implement solutions.

As specialists in infrastructure, information, physical and corporate security services, we approach security from every angle. Our security risk assessment methodology begins with an in-depth security review which includes:

- An assessment of current areas of exposure and any past security incidents to identify potential vulnerabilities.
- Interviews with employees and other key individuals for critical insights and information about situations, policies and procedures.
- A gap analysis to isolate areas, where your security program does not meet industry best practices.
- Recommendations that will mitigate any areas of vulnerability to reduce your risk.

CONSULTING

High-level event security planning and management.

Our team has decades of experience developing, organizing and implementing event-specific security plans for everything from discreet private events, to major celebrations, to highly publicized conferences and high-profile spectator events. Many of our professionals have served in law enforcement, the military and various government agencies in addition to managing security for organizations in diverse sectors internationally.

TRAINING

Security awareness, high-risk training and crisis management.

Risk mitigation and emergency planning are key to helping your organization plan for the unexpected. We can help train your team by providing resources that cover such topics as security awareness, high-risk training and crisis management. In addition to precise planning, we can offer tabletop exercises and skills development to reduce the impact of a critical incident—and potentially save lives in the process.

CRISIS MANAGEMENT PLANNING AND IMPLEMENTATION

One-stop shop for expert, on-site assistance for any emergency.

Out of nowhere, a crisis strikes. Think of natural disasters, business interruptions, criminal or malfeasance perpetrated by individuals, or violent political activity. Do your business leaders and employees know how to react to an active shooter situation, political or social unrest, a medical emergency or a hazmat incident?

We have the resources and know-how to quickly dispatch expert on-site assistance for any emergency. Our vetted consultants, business partners and in-house leadership can support your organizations both at home and abroad. With diverse skill sets, our experts can promptly respond to your needs and deliver the best crisis management and emergency response support internationally.

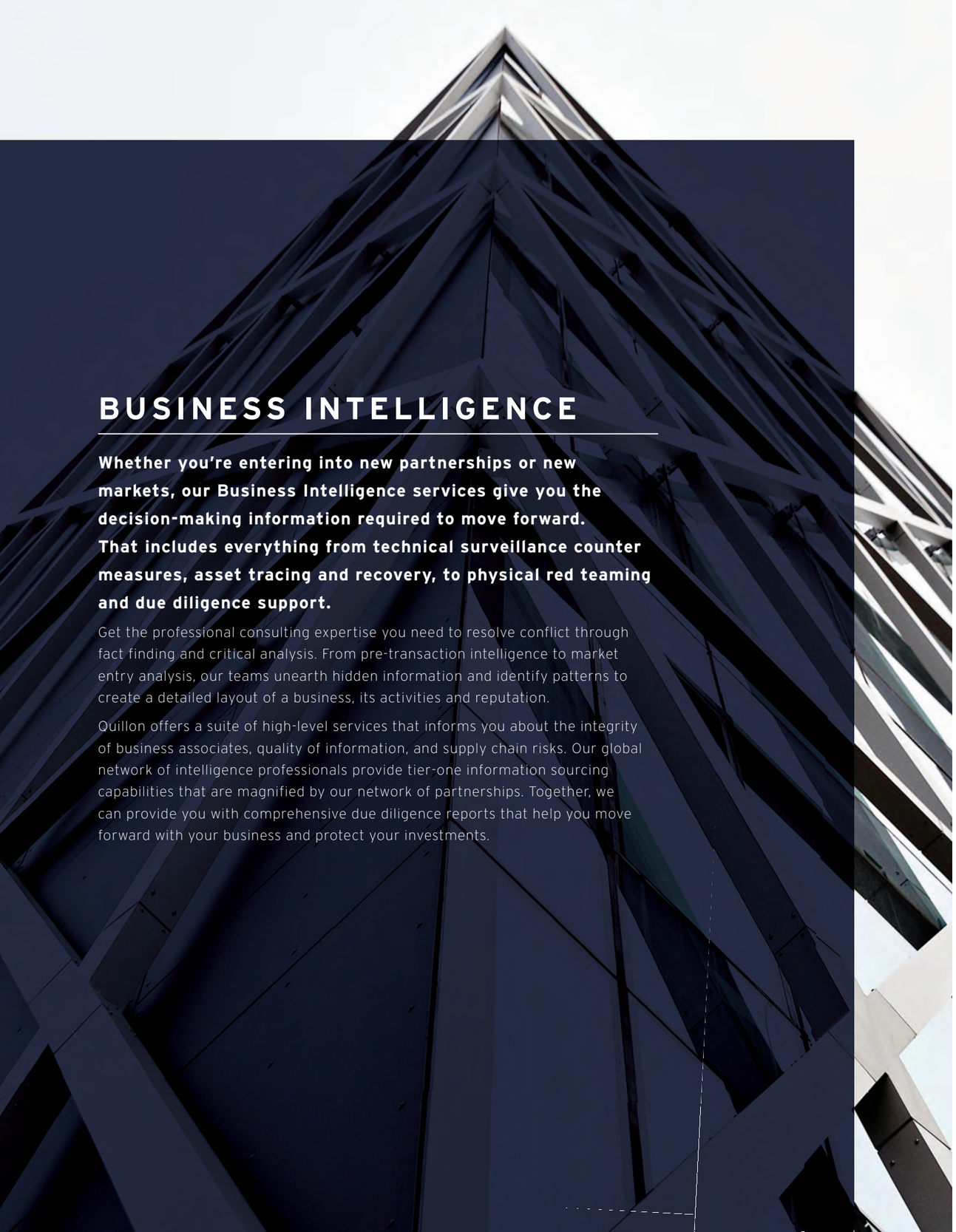
BUSINESS CONTINUITY PLANNING AND IMPLEMENTATION

Risk analysis for business and critical activities.

Anything that affects your facilities, operations or people can put your business continuity at risk. There are natural disasters like hurricanes that stall shipments of critical components, infrastructure failures like overtaxed power grids, as well as civil unrest or labour strikes.

Our team of experts can conduct a risk analysis of business groups and properties to understand your business and critical activities. We highlight any weaknesses in your existing business continuity and disaster recovery plans and recommend updates based on industry best practices.

QUILLON | STRENGTH IN SERVICE



BUSINESS INTELLIGENCE

Whether you're entering into new partnerships or new markets, our Business Intelligence services give you the decision-making information required to move forward. That includes everything from technical surveillance counter measures, asset tracing and recovery, to physical red teaming and due diligence support.

Get the professional consulting expertise you need to resolve conflict through fact finding and critical analysis. From pre-transaction intelligence to market entry analysis, our teams unearth hidden information and identify patterns to create a detailed layout of a business, its activities and reputation.

Quillon offers a suite of high-level services that informs you about the integrity of business associates, quality of information, and supply chain risks. Our global network of intelligence professionals provide tier-one information sourcing capabilities that are magnified by our network of partnerships. Together, we can provide you with comprehensive due diligence reports that help you move forward with your business and protect your investments.

TECHNICAL SURVEILLANCE COUNTERMEASURES (TSCM)

Professional TSCM for government, military, businesses, non-profits, executives, high-risk individuals and residential clients.

TSCM can be described as electronic bug detection, bug sweeping and/or counter surveillance. Wiretaps and various other eavesdropping equipment are readily accessible and continue to be more discrete, making the risk of personal and professional privacy much more difficult to control. Using the most advanced equipment available, our highly skilled professionals have the ability to detect "bugs" in buildings, vehicles, communications devices, network systems, and more.

ASSET TRACING AND RECOVERY

Tracing funds and identifying assets through complex money laundering schemes and corporate structures.

The satisfactory resolution of commercial disputes, or the recovery of the proceeds of fraud and embezzlement, frequently depends on successfully tracing and recovering assets. The location and ownership of those assets are often obscured through complex corporate, nominee or trust structures, and disbursed across multiple jurisdictions.

Our experts penetrate efforts to shield cash, real estate, corporate holdings, financial instruments, commodities, and other tangible and intangible assets from discovery. Our findings have helped clients establish the asset position of parties in contract disputes, enforce international arbitration awards, and recover assets in the aftermath of litigation and arbitration, complex frauds and banking collapses.

Our global engagement teams are made up of specialists in investigative research, forensic accounting, financial analysis, intelligence analysis, and cyber security. Working as an integrated unit, we are particularly effective at solving cross-border cases.

Successful asset tracing and recovery almost always occurs as part of a larger legal strategy and ensures that our efforts are focused on those assets which are of the most strategic value. Our experience working with law firms and general counsel makes us well-versed in identifying, compiling and preparing evidence that will stand up to scrutiny in a variety of legal proceedings and across jurisdictions.

PHYSICAL RED TEAMING

Physical penetration testers, known as a Red Team, are highly trained individuals who infiltrate secure environments employing techniques accomplished attackers use.

While companies worldwide continue to focus on incorporating security controls to safeguard computer systems from hackers, physical security should never be dismissed as a lesser problem. Many security breaches occur when attackers take advantage of one or more physical security deficiencies. Physical security penetration testing is one approach that organizations can use to improve their security controls.

Disgruntled ex-employees, crime rings and other nefarious entities employ sophisticated attack techniques and methods to exploit these deficiencies when attempting to gain unauthorized access to a company's assets and facilities.

Once they have breached a trusted environment, attackers may steal hard assets, intellectual property or otherwise cause serious disruptions.

Physical penetration testing provides real-world exploratory trials of how effective a company's physical security methods are when it comes to protecting equipment, data, and personnel. After discussing your methods with a security consultant, your site will be inspected by professionals who carefully evaluate and note vulnerabilities that are open to exploitation by attackers.

Primary objectives of physical penetration tests include assessing the ability of current physical security controls to prevent penetration by bad actors and actually testing these controls to determine their efficacy.

CYBER RISK MANAGEMENT

Securing information, networks and companies.

Together with our partners, we help you embrace digitization and digital transformation with confidence. This means helping you get value out of your digital investments by securing information, networks and companies with innovative cybersecurity products and services.

OFFENSIVE SECURITY

Concerned about the rise of cyber threats to network security, web applications, devices, servers, peripherals, and even people and physical buildings? Let us identify your real-world cybersecurity issues before they occur.

- **Penetration Testing (pen test) -** We work to identify your organization's security vulnerabilities through a systematic pen test process. This may focus on your networks, applications, physical facilities, human assets, and more. If left undetected, criminals and other malicious parties could exploit vulnerabilities to gain access to sensitive information or even take over entire systems.

  Our pen tests include simulated cyber-attacks, all developed by highly trained information security experts. Not only will our pen testing uncover and document cybersecurity problems, but the security assessment will provide risk assessments and effective security controls to eliminate vulnerabilities.
- **Red Teaming (ethical hacking) -** We crreate a full-scope, multi-layered attack simulation designed to measure how well a company's people and networks, applications, and physical security controls can withstand an attack from a real-life adversary.

A thorough red team test will expose vulnerabilities and risks regarding:

- **Technology and Information Security –** Networks, applications, routers, switches, appliances, sensitive data, phishing, etc.
- **People –** Staff, independent contractors, departments, business partners, etc.
- **Physical –** Offices, warehouses, substations, data centers, buildings, etc

LET US IDENTIFY YOUR REAL-WORLD CYBERSECURITY ISSUES BEFORE THEY OCCUR.

DEFENSIVE SECURITY

Experience has shown that no individual mitigation can stop all cyber threats, but together—when thoughtfully layered—they mitigate against a wide variety of threats while incorporating redundancy in the event one mechanism fails.

We apply the Defense in Depth (DiD) information security approach in which security mechanisms and controls are thoughtfully layered throughout a computer network to protect the confidentiality, integrity, and availability of the network and the data within. Our strategy may include these (and other) security best practices, tools, and policies

Firewalls – software or hardware appliances that control network traffic through access or deny policies or rules. These rules include black or whitelisting IP addresses, MAC addresses, and ports. There are also application-specific firewalls, such as Web Application Firewalls (WAF) and secure email gateways that focus on detecting malicious activity directed at a particular application.

Intrusion Prevention or Detection Systems (IDS/IPS) – an IDS sends an alert when malicious network traffic is detected whereas an IPS attempts to prevent and alert on identified malicious activity on the network or a user's workstation. These solutions base recognition of attacks on signatures of known malicious network activity.

Endpoint Detection and Response (EDR) software or agents reside on the client system (e.g. a user's laptop or mobile phone) and provide antivirus protection, alert, detection, analysis, threat triage, and threat intelligence capabilities. These solutions run on rulesets (i.e. signatures or firewall rules) or heuristics (i.e. detection of anomalous or malicious behaviors).

Network Segmentation is the practice of splitting a network into multiple sub-networks designed around business needs. For example, this often includes having sub-networks for executives, finance, operations, and human resources. Depending on the level of security required, these networks may not be able to communicate directly. Segmentation is often accomplished through the use of network switches or firewall rules.

The Principle of Least Privilege requires policy and technical controls to only assign users, systems, and processes access to resources (networks, systems, and files) that are absolutely necessary to perform their assigned function.

Strong Passwords are a critical authentication mechanism in information security. Modern password guidance involves using multifactor authentication for any account of value, using a phrase with multiple words, and not reusing passwords.

Patch Management is the process of applying updates to an operating system, software, hardware, or plugin. Often, these patches address identified vulnerabilities that could allow CTAs unauthorized access to information systems or networks.

PROTECTIVE SERVICES

A wide range of offerings, from professional front-of-house experience for concierge and reception, to industrial and construction sites, commercial and private locations, executive/personal protection and non-core policing services.

Our security protective services include:

- Uniformed guarding
- Managed protective services
- Non-core law enforcement services
- Executive/personal protection

We also have the ability to provide managed protective services globally. This service allows Quillon to provide protective services for our international clients anywhere in the world through our vetted partners.

Our personnel are fully trained and licensed to ensure we meet the highest standards of quality in the industry.

We utilize state-of-the-art security guard software to maintain accountability through effective GPS tracking and reporting and offer clients a range of data analytics.

WE VIEW SECURITY THROUGH A LENS OF INTEGRITY AND ACTIVELY ENGAGE WITH THE PEOPLE WHO ARE UNDER OUR TRUSTED CARE.

LET'S START THE CONVERSATION.

Get in touch to discuss your security challenges.

Quillon offers measurable risk reduction against all types of vulnerability. Whether protecting properties, bank accounts or reputations, we actively engage with the people who are under our trusted care

Quillon

E: info@quillon.ca

O: 1 877 QUILLON

W: quillon.ca

quillon