

جامعة ميدأوشن
Midocean University

كلية الإدارة | College of Management

قسم: إدارة المخاطر
Department of: Risk Management

استراتيجيات الحد من مخاطر الأطراف الثالثة في بيئات الأعمال المعاصرة
Strategies for Mitigating Third-Party Risks in Modern Project Environments

إعداد الطالب: محمد الراجح

العام الدراسي: 2025 / 2026

المنهجية: البحث النوعي التحليلي | (TPRM) المجال: إدارة مخاطر الأطراف الثالثة

فهرس المحتويات | Table of Contents

المستخلص / Abstract	3
المقدمة / الفصل الأول: Introduction	4
الفصل الثاني: الدراسات السابقة / Literature Review	5
الفصل الثالث: الإطار النظري / Theoretical Framework	6
الفصل الرابع: المنهجية / Methodology	8
الفصل الخامس: تصنيف المخاطر / Risk Taxonomy	9
الفصل السادس: دورة حياة إدارة المخاطر / TPRM Lifecycle	11
الفصل السابع: الحوكمة والامتثال / Governance & Compliance	13
الفصل الثامن: دراسات الحالة / Case Studies	15
الفصل التاسع: التقنيات الحديثة / Technology & Innovation	17
الفصل العاشر: النتائج / Results & Discussion	18
الفصل الحادي عشر: التوصيات / Recommendations	19
الفصل الثاني عشر: الخاتمة / Conclusion	20
المراجع / References	21

Abstract | المستخلص

المستخلص باللغة العربية

شكّل الانفتاح الواسع على شبكات الموردين الخارجيين تحولاً جوهرياً في طبيعة المخاطر التي تواجهها المنظمات المعاصرة. فمع توسّع نطاق الاستعانة بالمزودين الخارجيين لتنفيذ وظائف حيوية، باتت حدود المخاطر المؤسسية تمتد لتشمل كيانات خارج نطاق السيطرة المباشرة، مما أفرز ضرورة ملحة لتطوير منهجيات متطورة لإدارة هذه المخاطر بفاعلية. تتناول هذه الدراسة منظومة المخاطر المتشعبة الناجمة عن الاعتماد على الموردين الخارجيين، وتشمل: التهديدات السيبرانية، والتعطلات التشغيلية، والهشاشة المالية، والإشكاليات التنظيمية. ويستوقف النظر بصفة خاصة التأثير التضاعفي الذي يُفرزه تعدد طبقات سلاسل التوريد، حيث يُسهم كل مورد جديد في إضافة طبقة مخاطر يصعب الإحاطة بها والتحكم فيها.

تخلص الدراسة إلى بناء نموذج متجدد ومرن لإدارة مخاطر الأطراف الثالثة، يقوم على ثلاثة ركائز: متابعة الموردين في الوقت الفعلي، وتدرّج الحوكمة وفق مستويات المخاطر، وتعزيز التكامل المؤسسي بين مختلف الأقسام المعنية. الكلمات المفتاحية: إدارة مخاطر الأطراف الثالثة، مخاطر الموردين، الأمن السيبراني، سلاسل التوريد، المراقبة المستمرة، الثقة الصفريّة، الحوكمة، الامتثال.

Abstract in English

The growing reliance on external vendor networks has fundamentally reshaped the risk landscape facing contemporary organizations. As businesses assign critical operational tasks to outside parties, their exposure to risks originating beyond direct organizational control has grown considerably. This shift compels a more sophisticated and proactive approach to managing relationships with third-party providers.

This study examines the wide spectrum of risks that emerge from vendor dependency, spanning cybersecurity threats, service interruptions, financial vulnerabilities, and regulatory exposure. Particular attention is paid to the compounding effect created by layered supply chains, where each additional vendor tier introduces risk dimensions that are difficult to map and control.

The study proposes a dynamic and continuously adaptive model for third-party risk management, anchored in real-time vendor oversight, risk-proportionate governance, and cross-functional organizational integration. The model acknowledges that vendor risk profiles are not static, requiring sustained reassessment rather than isolated periodic reviews.

Keywords: Third-Party Risk Management, Vendor Risk, Cybersecurity, Supply Chain, Continuous Monitoring, Zero Trust, Governance, Compliance.

Chapter One: Introduction | الفصل الأول: المقدمة

1.1 Background and Context | السياق العام

لا يمكن فهم طبيعة المؤسسة الحديثة بمعزل عن شبكة علاقاتها مع الموردين الخارجيين. فعلى مدى العقود الماضية، تحول الاستعانة بمصادر خارجية من خيار تكتيكي إلى ركيزة استراتيجية راسخة، تشمل قطاعات حيوية كخدمات الحوسبة السحابية، وإدارة الأمن، وخدمات العملاء، ومعالجة الرواتب.

وعلى الرغم من المنطق الاقتصادي الداعم لهذا النهج، الذي يُتيح الوصول إلى الكفاءات المتخصصة وخفض التكاليف، فإنه يُفرز في الوقت ذاته مداخل جديدة للمخاطر. فكل مورد يحمل معه نموذج حوكمة مختلفاً، وسياسة أمنية خاصة، وأولويات أعمال قد تتعارض مع متطلبات المنظمة المتعقدة.

The modern enterprise cannot be fully understood without examining its external vendor ecosystem. Over the past two decades, outsourcing has evolved from a tactical option into a core strategic pillar, spanning critical areas such as cloud computing, managed security, customer service, and payroll processing. While the economic rationale is compelling, each vendor relationship introduces a distinct entry point for risk, carrying its own governance model, security posture, and business objectives that may diverge from those of the contracting organization.

1.2 Problem Statement | مشكلة الدراسة

تكمن الإشكالية الجوهرية في اعتقاد سائد بأن الموردين يظلون على نفس مستوى الموثوقية والامتثال طوال فترة تعاملهم مع المنظمة. وهذا الافتراض يقود إلى منح الموردين صلاحيات وصول ممتدة دون إعادة تقييم دورية كافية، مما يُهيئ بيئة خصبة لتضاعد المخاطر دون إنذار مسبق.

يتفاقم هذا الوضع في سياق تتداخل فيه سلاسل التوريد وتتشعب، حيث يتعاقد الموردون الأساسيون بدورهم مع موردين من مستويات أدنى، مما يُفضي إلى مخاطر مركبة تفوق قدرة أنظمة الرقابة التقليدية على تتبعها.

The central problem lies in the prevalent assumption that vendors maintain consistent reliability and compliance throughout their engagement lifecycle. This belief often leads organizations to extend access privileges without adequate periodic reassessment, creating an environment where risks can escalate undetected. The complexity intensifies in layered supply chains, where primary vendors subcontract to lower-tier providers, generating compounded risks that exceed the capacity of conventional monitoring systems.

1.3 Research Objectives | أهداف الدراسة

- رصد وتصنيف الفئات الرئيسية للمخاطر الناشئة عن علاقات الأطراف الثالثة في البيئات المؤسسية المعاصرة

- تقييم مدى كفاية الأطر المعيارية الدولية القائمة في معالجة هذه المخاطر بصورة شاملة وفعالة
- استخلاص دروس عملية من حوادث موثقة في قطاعات متنوعة تُبرز ثغرات إدارة مخاطر الموردين
- بناء نموذج متجدد ومتكيف لإدارة مخاطر الأطراف الثالثة يواكب ديناميكية بيئة الأعمال الرقمية
- تقديم توصيات قابلة للتطبيق الفعلي تُرشد المؤسسات نحو حوكمة أكثر صرامة وفعالية

1.4 | نطاق البحث وحدوده Scope and Limitations

يتمحور هذا البحث حول المنظمات متوسطة وكبيرة الحجم العاملة في قطاعات خاضعة للتنظيم كالخدمات المالية والرعاية الصحية وتقنية المعلومات. يعتمد البحث منهج التحليل النوعي للمصادر الثانوية، بما تشمله من الأدبيات الأكاديمية المحكّمة، والتقارير المهنية، ودراسات الحالة الموثقة.

This research centers on medium-to-large organizations operating in regulated sectors including financial services, healthcare, and information technology. The study adopts a qualitative analytical methodology drawing on peer-reviewed academic literature, professional industry reports, and documented case studies.

Chapter Two: Literature Review | الفصل الثاني: الدراسات السابقة

Evolution of Academic Research | مسار تطور البحث العلمي في هذا الميدان 2.1

شهد الاهتمام البحثي بمخاطر الأطراف الثالثة تصاعداً ملحوظاً في السنوات الأخيرة، مدفوعاً بتضايف عاملين رئيسيين: تنامي حوادث اختراق سلاسل التوريد، وتصاعد الضغوط التنظيمية الدولية. وقد انتقل البحث في هذا الميدان من التركيز الضيق على الأبعاد التعاقدية والمالية، إلى رؤية شاملة تضم الأبعاد التقنية والأمنية والتنظيمية والسلوكية.

Academic interest in third-party risk has grown markedly in recent years, driven by the convergence of two key forces: the rise in supply chain breach incidents and mounting international regulatory pressure. Research in this area has shifted from a narrow focus on contractual and financial dimensions to a comprehensive perspective encompassing technical, security, regulatory, and behavioral factors.

Existing International Frameworks | الأطر والمعايير الدولية القائمة 2.2

منظومة متكاملة لإدارة أمن المعلومات، تشمل في ضمن اشتراطاتها التعامل المنظم مع ISO/IEC 27001 يُقدم معيار مخاطر الموردين. في المقابل، يعتمد الإطار الإرشادي للأمن السيبراني الصادر عن المعهد الوطني للمعايير والتقنية الأمريكي خمس وظائف محورية: التعرف على المخاطر، والحماية منها، والكشف عنها، والاستجابة لها، والتعافي من آثارها. فتلزم المنظمات بالمسؤولية الكاملة عن كيفية تعامل معالجي البيانات (GDPR)، أما اللائحة الأوروبية لحماية البيانات من الأطراف الثالثة مع المعلومات الشخصية، مما يُضاف إلى حزمة واسعة من الأطر التنظيمية القطاعية المتخصصة.

The ISO/IEC 27001 standard provides an integrated information security management system that includes structured requirements for managing vendor-related risks. The NIST Cybersecurity Framework operates through five core functions: identifying risks, protecting against them, detecting them, responding to incidents, and recovering from impacts. The GDPR places full accountability on organizations for how their third-party data processors handle personal information, complementing a broad range of sector-specific regulatory frameworks.

Gaps in Current Literature | الفجوات في الأدبيات الحالية 2.3

يكشف استعراض الأدبيات عن قصور واضح في التعامل مع مخاطر الموردين من الدرجة الرابعة وما يليها، حيث تتوقف معظم الدراسات عند العلاقة المباشرة مع المورد الأول. كما أن النماذج النظرية كثيراً ما تفترض مستوى من النضج المؤسسي والتعاون من الموردين لا يعكس الواقع الفعلي في كثير من المنظمات.

A clear gap emerges in the literature regarding fourth-party and beyond vendor risks, as most studies halt at the direct vendor relationship. Theoretical models also frequently

assume levels of organizational maturity and vendor cooperation that do not accurately reflect operational realities across diverse organizations.

Chapter Three: Theoretical Framework | الفصل الثالث: الإطار النظري

Agency Theory and Vendor Dynamics | نظرية الوكالة وتوترات علاقة المورد 3.1

توفر نظرية الوكالة عدسة تحليلية ذات قيمة لفهم ديناميكيات العلاقة بين المنظمة والمورد. ففي هذه العلاقة، تُفوض المنظمة (بوصفها موكلًا) مهامًا جوهرية إلى المورد (بوصفه وكيلًا)، مما يُفرز فجوة معلوماتية هيكلية: فالمورد يعرف بالتفصيل أوضاعه الداخلية وقدراته ومخاطره، بينما لا تملك المنظمة إمكانية التحقق المستقل من هذه المعطيات.

هذه الفجوة تُهيئ ظروفاً لنوعين من الإشكاليات: الاختيار الخاطئ قبل التعاقد، حيث تنتهي المنظمة إلى اختيار مورد يحمل نقاط ضعف خفية، والمخاطرة الأخلاقية بعد التعاقد، حيث يُخفف المورد التزاماته بالأمن والجودة عقب تأمين العقد.

Agency theory offers a valuable analytical lens for understanding the organizational-vendor relationship. In this dynamic, the contracting organization acts as a principal delegating core tasks to a vendor as agent, creating a structural information gap. The vendor possesses detailed knowledge of its internal conditions, capabilities, and exposures that the organization cannot independently verify. This gap enables two categories of problems: pre-contractual adverse selection, where the organization inadvertently partners with a vendor harboring hidden weaknesses; and post-contractual moral hazard, where the vendor gradually reduces its security and quality investments after securing the contract.

Systems Thinking Approach | مقاربة التفكير المنظومي لمخاطر سلاسل التوريد 3.2

تمتلك سلاسل التوريد المعاصرة خصائص الأنظمة التكميفية المعقدة: تتفاعل أجزاؤها بصورة غير خطية، وتتضافر تأثيراتها بطرق يصعب توقعها مسبقاً. وهذا يعني أن التحليل الثنائي للعلاقة مع كل مورد بصورة منفردة يُغفل الصورة الأشمل لشبكة المخاطر المتشابكة.

يدعو منهج التفكير المنظومي إلى تحليل مخاطر شبكة الموردين بوصفها كلاً متكاملًا، عبر رسم خرائط الاعتماديات المتبادلة وتحديد نقاط الهشاشة البنوية التي قد تُعرض المنظمة لمخاطر متسلسلة.

Contemporary supply chains exhibit the properties of complex adaptive systems: their components interact nonlinearly, and their effects compound in ways that are difficult to anticipate. This means that bilateral analysis of individual vendor relationships overlooks the broader web of interconnected risks. A systems thinking approach advocates analyzing the vendor network as an integrated whole, mapping mutual dependencies and identifying structural vulnerabilities that could expose the organization to cascading risks.

Continuous Monitoring Model | نموذج المراقبة المستمرة والإدارة الديناميكية 3.3

يُفترض في هذه الدراسة نموذج متجدد لإدارة مخاطر الأطراف الثالثة يتجاوز نمط التقييم الدوري المنقطع، ويتأسس على أربعة محاور عملية:

- الرصد اللحظي: بناء قدرات تقنية تُتيح للمنظمة مواكبة التحولات في المشهد المخاطري للموردين بصورة آنية ومستمرة
- التسجيل الديناميكي: تحديث مستمر لمستويات مخاطر الموردين استناداً إلى المعطيات الجديدة بدلاً من الاكتفاء بالتقييمات السنوية
- التناسب في الاستجابة: ضبط كثافة المراقبة والرقابة بما يتناسب مع مستوى المخاطر الفعلي لكل مورد
- الحوار التشاركي: بناء علاقات تعاونية مستدامة مع الموردين تتجاوز الإطار التعاقدى الجامد

Chapter Four: Methodology | الفصل الرابع: المنهجية

4.1 Research Design | التصميم البحثي

تعتمد هذه الدراسة المنهج النوعي التحليلي، الذي يُلائم طبيعة الأسئلة البحثية الاستكشافية والتفسيرية. يسعى البحث إلى بناء فهم عميق للكيفية التي تُدرك بها المنظمات مخاطر الأطراف الثالثة وتتعامل معها في السياقات التشغيلية الواقعية، بدلاً من الاكتفاء بقياسها عبر مؤشرات إحصائية كمية.

This study adopts a qualitative analytical methodology suited to the exploratory and interpretive nature of the research questions. The aim is to develop a deep understanding of how organizations perceive and handle third-party risks within real operational contexts, rather than reducing them to quantitative indicators.

4.2 Data Sources | مصادر البيانات

اعتمدت الدراسة على ثلاث فئات من المصادر الثانوية: الأدبيات الأكاديمية المحكّمة في مجالات أمن المعلومات وإدارة المخاطر وإدارة سلاسل التوريد، والتقارير الصناعية والأوراق البحثية الصادرة عن مؤسسات متخصصة، فضلاً عن دراسات الحالة التفصيلية لحوادث مخاطر الموردين الموثقة في قطاعات مختلفة.

The study draws on three categories of secondary sources: peer-reviewed academic literature spanning information security, risk management, and supply chain management; industry reports and research papers from specialized institutions; and detailed case studies of documented vendor risk incidents across various sectors.

4.3 Validity and Reliability | المصداقية والموثوقية

لتعزيز مصداقية النتائج، اعتمدت الدراسة أسلوب التثليث المنهجي، وهو المقارنة المنتظمة بين ما تقوله الأدبيات الأكاديمية وما تُفصح عنه الممارسات الصناعية وما تكشفه شواهد دراسات الحالة. وعند تباين المصادر، يُشار إلى مواطن الخلاف ويُتناول تفسيرها بمنهجية نقدية.

To strengthen the credibility of findings, the study employs methodological triangulation, systematically comparing academic literature, industry practice, and case study evidence. Where sources diverge, points of disagreement are identified and examined through critical analysis.

Chapter Five: Risk Taxonomy | الفصل الخامس: تصنيف المخاطر

5.1 Cybersecurity Risks | المخاطر السيبرانية

تحتل المخاطر السيبرانية مرتبة الصدارة في حوادث الأطراف الثالثة الموثقة. فالموردون المخوّلون بالوصول إلى أنظمة المنظمة أو شبكاتها أو بياناتها يُمثلون نقاطاً محتملة لاختراق الجهات الخبيثة. وتدرج ضمن هذه الفئة أربعة أنماط فرعية متميزة:

- اختراق سلسلة توريد البرمجيات: تلويث البرمجيات أو التحديثات التي يُصدرها المورد بشيفرات ضارة تُصيب المنظمات المستخدمة لها دون علمها
- سرقة بيانات الاعتماد: الاستيلاء على هويات موظفي المورد الرقمية واستغلالها للتسلل إلى بيئة المنظمة
- تسريب البيانات: انكشاف المعلومات الحساسة التي تتدفق إلى المورد لأغراض مشروعة نتيجة إخفاقاته الأمنية
- تمدد الغدية الخبيثة: انتشار برامج الغدية عبر روابط الشبكة المشتركة من بيئة المورد إلى المنظمة المتعاقدة

5.2 Operational Risks | المخاطر التشغيلية

حين يُخفق الموردون في الوفاء بالتزاماتهم الخدمية، تتجاوز التداعيات النطاق الداخلي لتتأثر عمليات المنظمة بأكملها. وتبرز أبرز مسبباتها في: ضعف طاقة المورد الاستيعابية، والاعتماد المفرط على أفراد بعينهم، والتمركز الجغرافي للعمليات في مناطق هشة، وقصور خطط استمرارية الأعمال.

When vendors fail to meet their service commitments, the consequences extend beyond the vendor relationship to affect the organization's overall operations. Key drivers include limited vendor capacity, excessive dependency on specific personnel, geographic concentration of operations in vulnerable areas, and inadequate business continuity planning.

5.3 Financial Risks | المخاطر المالية

صحة المورد المالية ليست معطًى ثابتاً، بل تتقلب مع تغيرات السوق والإدارة والمنافسة. ويُعدّ المورد الذي يمر بضائقة مالية مصدراً مزدوجاً للمخاطر: فهو يُقلّص استثماراته في الأمن والجودة من جهة، وقد ينهار مفاجئاً محدثاً فجوات خدمية صعبة الترقيع من جهة أخرى. وتأخذ هذه المخاطر طابعاً ثنائي الاتجاه، إذ يمكن أن تُفضي إخفاقات المورد إلى تعريض المنظمة لمطالبات تعويضية وعقوبات تنظيمية.

A vendor's financial health is not a fixed parameter but fluctuates with market shifts, management changes, and competitive pressures. A vendor experiencing financial distress poses dual risks: it reduces investments in security and quality, and may suddenly collapse, leaving difficult-to-fill service gaps. These risks are bidirectional, as

vendor failures can expose the contracting organization to compensation claims and regulatory penalties.

5.4 مخاطر الامتثال التنظيمي | Regulatory Compliance Risks

تُبقى التشريعات الحديثة المسؤولية التنظيمية على عاتق المنظمة المتعاقدة بصرف النظر عن مصدر الإخلال. فإذا أُخلّ المورد بمتطلبات حماية البيانات، أو سلامة المعاملات المالية، أو أمن الأنظمة الحرجة، تتحمل المنظمة في الغالب عواقب قانونية ومالية مباشرة.

Modern legislation maintains regulatory accountability on the contracting organization regardless of the source of the violation. If a vendor breaches data protection requirements, financial transaction integrity, or critical systems security, the organization typically bears direct legal and financial consequences.

5.5 المخاطر السمعية | Reputational Risks

في عالم يتشكل فيه الوعي العام بسرعة عبر وسائل التواصل الاجتماعي والإعلام الرقمي، لا تُفرّق الجماهير في الغالب بين ما تُسببه المنظمة ذاتها وما ينشأ عن إخفاقات مورديها. وقد يُلحق ذلك ضرراً بالغاً بالسمعة المؤسسية، ينعكس على الاحتفاظ بالعملاء، واستقطاب المواهب، وثقة المستثمرين.

In a world where public awareness forms rapidly through social media and digital news, audiences rarely distinguish between what an organization causes directly and what results from its vendors' failures. This can inflict serious reputational damage, affecting customer retention, talent attraction, and investor confidence.

Chapter Six: TPRM | الفصل السادس: دورة حياة إدارة المخاطر Lifecycle

Vendor Identification and Risk Tiering | رصد الموردین وتدرّج المخاطر 6.1

ترتكز المرحلة التأسيسية على بناء جرد شامل وحيّ لجميع علاقات الأطراف الثالثة، مصنّفةً وفق عوامل المخاطر الجوهرية كحساسية البيانات المُتاحة، وأهمية الخدمات المقدمة، ودرجة التداخل التقني مع أنظمة المنظمة. يُمكن هذا التصنيف من توجيه الموارد المحدودة نحو الموردین الأعلى مخاطرةً بدلاً من توزيعها بصورة متساوية غير مُثمرة.

The foundational phase involves building a comprehensive, living inventory of all third-party relationships, classified according to key risk factors such as data sensitivity, service criticality, and degree of technical integration. This classification enables targeted allocation of limited resources toward higher-risk vendors rather than an inefficient equal distribution.

Pre-Onboarding Due Diligence | العناية الواجبة قبل الانضمام 6.2

قبل إبرام أي عقد، ينبغي إخضاع المورد المرتقب لمراجعة شاملة تتناسب في عمقها مع درجة مخاطره. وبالنسبة للموردین عالي الحساسية، تستلزم هذه المراجعة فحص شهادات الأمن، ونتائج اختبارات الاختراق، والبيانات المالية، وسجلات الامتثال، وإفادات العملاء الحاليين.

Before entering any contract, prospective vendors should be subjected to thorough review proportionate to their risk tier. For high-sensitivity vendors, this review encompasses security certifications, penetration test results, financial statements, compliance records, and references from existing clients.

Contracting and Legal Protections | التعاقد والحمايات القانونية 6.3

يُشكّل العقد الأداة القانونية الرئيسية لتوزيع المخاطر وتحديد الالتزامات. وينبغي أن يتضمن العقد الفغال: اشتراطات أمنية واضحة، وآليات إشعار فورية عند الانتهاكات، وصلاحيات تدقيق، ومعايير محددة لمستوى الخدمة، وأحكاماً تُنظّم استخدام المتعاقدين من الباطن.

The contract serves as the primary legal instrument for allocating risks and defining obligations. Effective contracts should include clear security requirements, timely breach notification mechanisms, audit rights, defined service level standards, and clauses governing the use of subcontractors.

6.4 المراقبة المستمرة وقياس الأداء | Ongoing Monitoring and Performance

تُمثل المتابعة المستمرة العمود الفقري لأي منظومة فعّالة لإدارة مخاطر الأطراف الثالثة. تشمل هذه المتابعة أدوات آلية لمراقبة الوضع الأمني الخارجي للموردين، وتقييمات هيكلية دورية، وفي حالة الموردين البالغين الحساسية، عمليات تفتيش ميداني.

Continuous monitoring forms the backbone of any effective third-party risk management system. This includes automated tools for tracking vendors' external security posture, periodic structured assessments, and for the most sensitive vendors, on-site inspection activities.

6.5 الاستجابة للحوادث المرتبطة بالموردين | Incident Response

ينبغي لكل مؤسسة أن تمتلك إجراءات استجابة للحوادث مُصمّمة خصيصاً لسيناريوهات الأطراف الثالثة، تتضمن: مسارات تصعيد واضحة، وبروتوكولات تواصل مع المورد، وآليات لتحليل الأسباب الجذرية واستخلاص الدروس عقب كل حادثة.

Every organization should maintain incident response procedures specifically designed for third-party scenarios, encompassing clear escalation paths, vendor communication protocols, and mechanisms for root cause analysis and lesson extraction following each incident.

6.6 إنهاء علاقة المورد | Vendor Offboarding

يحمل إنهاء علاقة المورد مخاطر محددة كثيراً ما تُستهان بها. فعملية الانفصال غير المنظمة قد تُبقي للمورد السابق صلاحيات وصول متبقية، أو بيانات لم تُحذف أو تُعاد، مما يُبقي باب المخاطرة مفتوحاً بعد انتهاء العلاقة التعاقدية.

Terminating a vendor relationship carries specific risks that are frequently underestimated. An unstructured separation process may leave residual access privileges with the former vendor or data that has not been deleted or returned, keeping the risk door open beyond the contractual relationship.

Chapter Seven: Governance and Compliance | الفصل السابع: الحوكمة والامتثال

Organizational Governance Structures | الهياكل المؤسسية للحوكمة 7.1

تستلزم حوكمة مخاطر الأطراف الثالثة وجود هياكل تنظيمية واضحة تتجاوز الحواجز التقليدية بين الأقسام. فكثيراً ما تُدار علاقات الموردين بصورة مجزأة بين المشتريات والتقنية والشؤون القانونية، دون تنسيق يضمن مستوىً متجانساً من الرقابة. تتميز المنظمات الرائدة بإنشاء وحدة متخصصة لإدارة مخاطر الأطراف الثالثة، تتمتع بتمثيل متعدد الأقسام ورعاية تنفيذية رفيعة.

Third-party risk governance requires organizational structures that transcend traditional departmental boundaries. Vendor relationships are often managed in fragmented ways across procurement, technology, and legal functions, without coordination ensuring a consistent oversight standard. Leading organizations establish dedicated TPRM units with cross-functional representation and senior executive sponsorship.

Regulatory Requirements | المتطلبات التنظيمية المقارنة 7.2

يتسم المشهد التنظيمي العالمي بالتنوع والتعقيد، ويشهد تشدداً متصاعداً في متطلبات الرقابة على الأطراف الثالثة:

ملاحظات	المتطلب الجوهرى	النطاق الجغرافى	الإطار التنظيمى
	ضمان الرقابة على معالجي البيانات وتوثيق العقود	الاتحاد الأوروبي	GDPR
	إدارة العلاقات مع الموردين ضمن منظومة أمن المعلومات	دولى	ISO 27001
	دمج إدارة مخاطر سلاسل التوريد فى منظومة الأمن السيبرانى	الولايات المتحدة	NIST CSF
	الرقابة على امتثال مزودى الخدمات لمعايير أمن البيانات	عالمى	PCI DSS
	إدارة مخاطر تقنية المعلومات لدى الأطراف الثالثة فى القطاع المالى	الاتحاد الأوروبي	DORA

Board-Level Oversight | الرقابة على مستوى القيادة العليا 7.3

لا يمكن اختزال مسؤولية حوكمة مخاطر الأطراف الثالثة فى المستويات التشغيلية. ففي ظل التحولات التنظيمية الراهنة، بات مجلس الإدارة يتحمل مسؤولية مباشرة عن كفاية منظومة إدارة هذه المخاطر، مما يستوجب الحصول على تقارير دورية. تعكس حالة محفظة الموردين وأبرز مخاطرها الناشئة.

Third-party risk governance responsibility cannot be confined to operational levels. Under current regulatory shifts, boards of directors bear direct accountability for the adequacy of these risk management systems, requiring regular reporting that reflects the state of the vendor portfolio and its most significant emerging risks.

Chapter Eight: Case Studies | الفصل الثامن: دراسات الحالة

8.1 SolarWinds (2020) | The SolarWinds Incident

تُجسّد هذه الحادثة ذروة التعقيد في مخاطر سلاسل توريد البرمجيات. تمكّن مهاجمون من الولوج إلى بيئة تطوير شركة المصنّعة لبرنامج مراقبة الشبكات، وأقحموا شيفرة ضارة في دورة البناء الاعتيادية للمنتج. وعندما وُزعت SolarWinds إلى آلاف الشركة التحديث الموقع رقمياً والموثوق به للعملاء، حمل معه البرنامج الخبيث المعروف بـ SUNBURST حول العالم.

ما يجعل هذه الحادثة استثنائية هو أن ناقل الهجوم كان قناة التحديث المشروعة بذاتها، مما جعل ضحاياها يُنصّبون الخطر بأيديهم داخل بيئاتهم. قُدّر عدد المتضررين بنحو 18,000 مؤسسة، من بينها وكالات حكومية أمريكية بالغة الحساسية.

This incident represents the apex of software supply chain risk complexity. Attackers penetrated the development environment of SolarWinds, a network monitoring software provider, and embedded malicious code into the routine product build cycle. When the company distributed the digitally signed and trusted update to customers, the malware known as SUNBURST was carried into thousands of organizations worldwide. What makes this incident exceptional is that the attack vector was the legitimate update channel itself, causing victims to install the threat by their own hand. The estimated number of affected organizations reached approximately 18,000, including highly sensitive U.S. government agencies.

الدروس المستخلصة:

- التحقق من سلامة سلاسل توريد البرمجيات يستلزم أدوات تشفيرية وسلوكية، ولا يكفي الاعتماد على ثقة المورد وحدها
- التحديثات البرمجية القادمة من الموردين تستحق معاملةً احترازية بصرف النظر عن ثقتهم المعتادة
- رصد الاتصالات الصادرة غير المعتادة يُعدّ خطأً دفاعياً فعّالاً ضد هذا النمط من الهجمات

8.2 Target (2013) | The Target Data Breach

كشف هذا الاختراق عن مفارقة صارخة: مؤسسة تجارية عملاقة تسقط ضحيةً لثغرة في مورد صغير لأنظمة التكييف. حصل لخدمات التدفئة والتبريد عبر حملة تصيد احتيالي، ثم Fazio Mechanical المهاجمون على بيانات اعتماد شركة ومنها تمكّنوا من التحرك جانبياً داخل الشبكة حتى بلغوا Target، وظفّوا هذه البيانات للنفاذ إلى بوابة الموردين في أنظمة نقاط البيع، حيث زرعوا برمجية تعمل على استخلاص بيانات الدفع لنحو 40 مليون عميل.

This breach exposed a striking paradox: a retail giant falling victim to a vulnerability in a small air conditioning systems vendor. Attackers obtained credentials from Fazio Mechanical through a phishing campaign, then used them to access Target's vendor portal and move laterally through the network until reaching point-of-sale systems, where

they planted malware that extracted payment data from approximately 40 million customers.

- مبدأ الحد الأدنى من المصالحات يجب تطبيقه بصرامة على جميع الموردين بصرف النظر عن طبيعة الخدمة
- عزل شبكة الموردين عن الأنظمة الحساسة ضرورة تقنية لا خيار اختياري
- المصادقة متعددة العوامل تُقيد الاستخدام الاحتياطي لبيانات اعتماد الموردين

8.3 Kaseya (2021) | The Kaseya Attack

كشف هذا الهجوم عن الإمكانية التدميرية لاختراق مزودي الخدمات المُدارة بوصفهم نقطة تمرکز استراتيجية للمهاجمين. المخصصة لإدارة البنية التحتية لدى مزودي الخدمات المُدارة، مما Kaseya VSA استغل المهاجمون ثغرات في منصة أتاح لهم نشر برامج الفدية بصورة متزامنة لدى آلاف العملاء النهائيين التابعين لهؤلاء المزودين، ليصل العدد المقدر للمتضررين إلى 1,500 مؤسسة في مختلف أنحاء العالم.

This attack revealed the destructive potential of compromising managed service providers as strategic attack hubs. Attackers exploited vulnerabilities in the Kaseya VSA platform used to manage IT infrastructure for managed service providers, enabling simultaneous ransomware deployment across thousands of end-client organizations, with estimated affected entities reaching 1,500 worldwide.

Chapter | الفصل التاسع: التقنيات الحديثة في إدارة مخاطر الأطراف الثالثة Nine: Technology & Innovation

9.1 Artificial Intelligence and Machine Learning | الذكاء الاصطناعي وتعلم الآلة

تُفتح تقنيات الذكاء الاصطناعي آفاقاً جديدة لتحسين منظومة إدارة مخاطر الأطراف الثالثة. فمعالجة اللغات الطبيعية تُمكن من استخلاص إشارات المخاطر المبكرة من المصادر غير المنظمة كالأخبار والتقارير التنظيمية. كما تستطيع نماذج التحليل التنبؤي اكتشاف أنماط في سلوك الموردين تسبق ظهور المخاطر الفعلية، مما يُتيح التدخل الاستباقي قبل تحوّلها إلى حوادث.

Artificial intelligence technologies open new horizons for enhancing third-party risk management. Natural language processing enables extraction of early risk signals from unstructured sources such as news and regulatory reports. Predictive analytics models can detect patterns in vendor behavior that precede actual risk emergence, enabling proactive intervention before they evolve into incidents.

9.2 Zero Trust Architecture | نموذج الثقة الصفرية في إدارة الوصول

يُقدّم نموذج الثقة الصفرية تحولاً جذرياً في منهجية إدارة صلاحيات الموردين: بدلاً من الثقة المبنية على الهوية المعتمدة سلفاً، تُنشأ كل جلسة وصول على أساس التحقق المستمر من الهوية وسلامة الجهاز والسياق. ويشمل ذلك التقطيع الدقيق للشبكة، وتوفير الوصول اللحظي عند الحاجة فقط، ومراقبة شاملة للجلسات، والتخلص التام من بيانات الاعتماد الدائمة.

The Zero Trust model represents a radical shift in vendor access management methodology: rather than trust built on pre-approved identity, each access session is established on the basis of continuous verification of identity, device integrity, and context. This includes micro-segmentation of the network, just-in-time access provisioning only when needed, comprehensive session monitoring, and complete elimination of persistent credentials.

9.3 Vendor Risk Rating Services | خدمات التقييم المستمر للموردين

نشأ نظام بيئي من خدمات تقييم مخاطر الموردين يعتمد على تحليل البيانات المتاحة للعموم لتوليد تقييمات أمنية مستمرة. وعلى الرغم من قيمتها كمؤشر إضافي، تجدر الإشارة إلى أن هذه الخدمات لا ترصد إلا جزءاً من الصورة الأمنية الشاملة للمورد، ولا ينبغي الاعتماد عليها بمعزل عن التقييمات الداخلية المباشرة.

An ecosystem of vendor risk rating services has emerged, relying on analysis of publicly available data to generate continuous security scores. Despite their value as supplementary indicators, it should be noted that these services capture only a portion of

the vendor's comprehensive security picture and should not be relied upon in isolation from direct internal assessments.

Chapter Ten: Results and Discussion | الفصل العاشر: النتائج والمناقشة

Key Findings | أبرز النتائج 10.1

يُخلص التحليل المنهجي لمصادر هذه الدراسة إلى خمسة أنماط متكررة تُصوّر الواقع الراهن لإدارة مخاطر الأطراف الثالثة

- تميل المنظمات إلى التقليل من تقدير عمق وتشابك اعتمادياتها على الموردين، خاصةً على المستويات الأبعد من المورد المباشر
- يوجد فجوة واضحة بين امتلاك سياسات إدارة مخاطر الموردين وبين التطبيق الفعلي المتسق لهذه السياسات على أرض الواقع
- تتمحور الفوارق الجوهرية بين المنظمات في التعامل مع الحوادث حول قدرتها على المتابعة المستمرة والكشف المبكر
- يعاني كثير من المنظمات من تشتت مسؤوليات حوكمة الموردين بين أقسام متعددة دون تنسيق فعال
- تتصاعد التوقعات التنظيمية باستمرار في معظم الولايات القضائية، مما يُضيق هامش التساهل في هذا الملف

Discussion | مناقشة النتائج 10.2

تُشير هذه النتائج مجتمعةً إلى أن العائق الرئيسي في هذا الميدان ليس نقص الأطر النظرية أو غموض المبادئ التوجيهية، بل يكمن في الهوة بين ما تنصّ عليه السياسات وما يحدث فعلياً على مستوى الممارسة اليومية. وتؤكد دراسات الحالة هو في TPRM المُحللة أن الحوادث الكبرى تستغل تحديداً هذه الهوة التنفيذية، مما يُرسّخ الفهم بأن بناء قدرات جوهره تحدّي مؤسسي وثقافي قبل أن يكون تقنياً.

These findings collectively indicate that the primary barrier in this domain is not a shortage of theoretical frameworks or ambiguity of guiding principles, but rather the gap between what policies prescribe and what actually occurs at the level of daily practice. The analyzed case studies confirm that major incidents specifically exploit this implementation gap, reinforcing the understanding that building TPRM capabilities is fundamentally an organizational and cultural challenge before being a technical one.

Chapter Eleven: Recommendations | الفصل الحادي عشر: التوصيات

بناءً على ما خلصت إليه هذه الدراسة من نتائج، تُقدّم التوصيات التالية مُرتبةً من الأكثر أساسية إلى الأكثر تقدماً:

1. Unified Vendor Registry | إنشاء سجل موحد وحّي للموردين

لا يمكن إدارة ما لا يُرى. وتبدأ أي منظومة فعّالة لإدارة مخاطر الأطراف الثالثة بامتلاك رؤية شاملة وحديثة لجميع العلاقات مع الموردين بما فيها المتعاقدون من الباطن، مع تحديد سمات المخاطر لكل منهم.

2. Risk-Tiered Classification | تطبيق منهجية تدرّج المخاطر

لا يستحق جميع الموردين مستوىً متماثلاً من الرقابة. ويستلزم التدرّج الفعّال للمخاطر بناء معايير واضحة لتصنيف الموردين وتكييف كثافة المراقبة وفق هذا التصنيف.

3. Contract Enhancement | تطوير العقود لتتضمن ضمانات أمنية متينة

ينبغي أن يُصبح العقد أداةً استراتيجية لإدارة المخاطر لا مجرد وثيقة تجارية. ويتطلب ذلك إدراج اشتراطات أمنية ملزمة، وآليات تدقيق، والتزامات واضحة بالإفصاح عن الحوادث.

4. Continuous Monitoring | الاستثمار في المراقبة المستمرة الآلية

يُوفر الجمع بين أدوات المراقبة الآلية والتقييمات الدورية المنتظمة طبقات دفاعية متكاملة، تُمكن المنظمة من الكشف المبكر عن التدهور في الوضع الأمني للموردين.

5. Zero Trust for Vendor Access | تطبيق مبادئ الثقة الصفيرية على وصول الموردين

ينبغي إعادة هيكلة صلاحيات وصول الموردين وفق مبادئ الثقة الصفيرية، مع إيلاء الأولوية لمبدأي الحد الأدنى من الصلاحيات والوصول في الوقت المناسب.

6. Cross-Functional Governance | بناء حوكمة متعددة الأقسام لإدارة مخاطر الموردين

يُعدّ التنسيق بين التقنية والأمن والمشتريات والشؤون القانونية والامتثال والأعمال شرطاً لا غنى عنه، مع تخصيص رعاية تنفيذية واضحة وإعداد تقارير دورية لمجلس الإدارة.

7. Vendor Incident Response Plans | صياغة خطط استجابة خاصة بحوادث الموردين

ينبغي أن تمتلك كل مؤسسة إجراءات موثقة ومُختبرة للتعامل مع سيناريوهات الحوادث المرتبطة بالموردين، تتكامل مع منظومة الاستجابة الأشمل للمؤسسة.

Chapter Twelve: Conclusion | الفصل الثاني عشر: الخاتمة

جاء اهتمام هذه الدراسة بإدارة مخاطر الأطراف الثالثة انعكاساً لأهمية تصاعدية يُسجلها هذا الملف في أجندات إدارة المخاطر المؤسسية. فمع توسع دائرة الاعتماد على الموردين الخارجيين، لم يعد بمقدور المنظمات معالجة هذه المخاطر كملحق على هامش منظومة الحوكمة، بل باتت جزءاً لا يتجزأ من استراتيجية الصمود والمرونة المؤسسية.

كشفت الدراسة أن المخاطر الناجمة عن علاقات الموردين متشعبة ومتداخلة، ولا تُحسن نمذجتها الأطر الخطية التقليدية. لم تكن نتائج ثغرات تقنية وحسب، بل كانت في Kaseya و Target و SolarWinds فالحوادث الكبرى كاختراقات جوهرياً استغلالاً للثقة والثغرات في منظومة حوكمة الموردين.

يُفترض في هذه الدراسة نموذج إدارة مخاطر متجدد يستبدل نمط التقييم الدوري بمتابعة مستمرة وديناميكية، يُكسب المنظمات الوعي الظرفي اللازم للكشف عن المخاطر ومعالجتها قبل أن تتحول إلى حوادث بالغة الأثر.

في المحصلة، بناء منظومة متينة لإدارة مخاطر الأطراف الثالثة هو في جوهره استثمار في القدرة المؤسسية، يحتاج إلى إرادة قيادية، وتخصيص موارد كافية، وترسيخ ثقافة الوعي بالمخاطر عبر مختلف طبقات المنظمة.

This study's engagement with third-party risk management reflects the growing prominence of this issue in institutional risk management agendas. As vendor dependency widens, organizations can no longer treat these risks as a peripheral governance concern, but must integrate them as a core component of resilience and institutional continuity strategy. The study reveals that risks arising from vendor relationships are multifaceted and interconnected, poorly modeled by traditional linear frameworks. The major incidents of SolarWinds, Target, and Kaseya were not merely technical failures, but fundamentally exploitations of trust and gaps in vendor governance systems. The continuous risk management model proposed here replaces periodic assessment cycles with sustained dynamic monitoring, equipping organizations with the situational awareness needed to detect and address risks before they escalate into high-impact incidents.

المراجع | References

المراجع الأجنبية | International References

- Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation*, 34(7), 342–353. <https://doi.org/10.1016/j.technovation.2014.02.001>
- Chopra, S., & Sodhi, M. (2014). Reducing the risk of supply chain disruptions. *MIT Sloan Management Review*, 55(3), 73–80.
- European Parliament. (2018). General Data Protection Regulation (GDPR) — Regulation (EU) 2016/679. Official Journal of the European Union.
- FireEye / Mandiant. (2020). Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims. Mandiant Intelligence Report.
- International Organization for Standardization. (2022). ISO/IEC 27001:2022 — Information Security, Cybersecurity and Privacy Protection. Geneva: ISO.
- Krebs on Security. (2014). Target Hackers Broke In Via HVAC Company. Security Investigation Blog.
- National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. NIST.
- National Institute of Standards and Technology. (2022). Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. NIST SP 800-161 Rev. 1.
- Payment Card Industry Security Standards Council. (2022). PCI DSS v4.0 — Payment Card Industry Data Security Standard.
- Ponemon Institute. (2022). 2022 Cost of a Data Breach Report. IBM Security.
- Verizon. (2023). 2023 Data Breach Investigations Report. Verizon Business.
- World Economic Forum. (2023). Global Cybersecurity Outlook 2023. World Economic Forum Insight Report.
- Zsidisin, G. A., & Ritchie, B. (Eds.). (2009). Supply Chain Risk: A Handbook of Assessment, Management, and Performance. Springer.

الملاحق | Appendices

الملحق أ: نموذج الاستبيان | Appendix A: Survey Instrument

القسم الأول: البيانات الأساسية | Section 1: Basic Information

- Job title and industry sector | المسمى الوظيفي والقطاع الذي تعمل فيه
- Organizational size by employee count | حجم المنظمة من حيث عدد الموظفين
- Number of currently active external vendors | عدد الموردين الخارجيين النشطين حالياً

القسم الثاني: الممارسات الحالية | Section 2: Current Practices

- Does your organization have a formal TPRM program? | هل يوجد في مؤسستك برنامج رسمي لإدارة مخاطر الأطراف الثالثة؟
- Which standards frameworks do you currently apply? | ما الأطر المعيارية المعتمدة لديكم؟
- How do you assess risk levels across different vendors? | كيف تُقيّمون مستوى مخاطر الموردين المختلفين؟
- How frequently are vendor reviews conducted? | ما تكرر إجراء مراجعات الموردين؟

القسم الثالث: التحديات والثغرات | Section 3: Challenges and Gaps

- What are the main obstacles to implementing TPRM? | ما أبرز العقبات التي تعترض تطبيق إدارة مخاطر الأطراف الثالثة؟
- Has your organization experienced incidents attributable to vendor risk failures? | هل تعرّضت مؤسستك لحوادث ناجمة عن إخفاقات في إدارة مخاطر الموردين؟