Predicts 2024: Geopolitics, SaaS and Generative AI Impact IT Vendor Risk

Published 6 December 2023 - ID G00802334 - 14 min read

By Analyst(s): Sundar Viswanathan, Ben Jepson, Ciaran Hudson, Tsuyoshi Ebina, Yoann Bianic

Initiatives: IT Vendor Ecosystems Management

> Disruption stemming from the shift to SaaS by enterprise software vendors, geopolitical climate, and GenAI will impact IT vendor risks. Sourcing, procurement and vendor management leaders should develop new perspectives and embrace change to mitigate risks and capitalize on opportunities.

Overview

Key Findings

- The geographical concentration of headquarters and service delivery locations for major cloud infrastructure and platform services (CIPS) and SaaS providers presents a geopolitical risk. Implications of access restrictions or supply chain reorganization by one or a handful of IT vendors in one political block could put thousands of businesses, millions of customers and billions of dollars at risk.

- The shift to subscription and SaaS-based offerings by major enterprise software providers has a direct impact on the business of other vendors in the software product ecosystem. For instance, third-party service providers and managed service providers that have traditionally maintained the clients of software product code and specialized infrastructure are getting disrupted as clients consume the software product and the underlying infrastructure as a service. This development necessitates a reassessment of vendor risks and portfolios.

- Rapid innovation in advanced contract analytics products using generative AI will accelerate adoption of already maturing use cases like automated contract review. To manage the volume growth in contract reviews due to evolving regulatory mandates, performance standards and licensing models organizations will look to technology to scale up.

Recommendations

- Mitigate geopolitical risks by addressing the headquarters and service delivery location concentration risks in your vendor portfolio.
- Assess the business strategies of vendors across the ecosystem to mitigate market exit risks.
- Evaluate generative AI (GenAI) for its ability to improve contract review efficiencies and automate license desk layers in the software asset management (SAM) function to reduce risk exposure.

Strategic Planning Assumptions

By 2027, geopolitical issues will increase the defaults in SaaS contract commitments, impacting over 50% of subscribers.

By 2028, one of the main third-party support providers will fail as software providers successfully move customers to subscription models, creating potential vendor ecosystem risks for organizations.

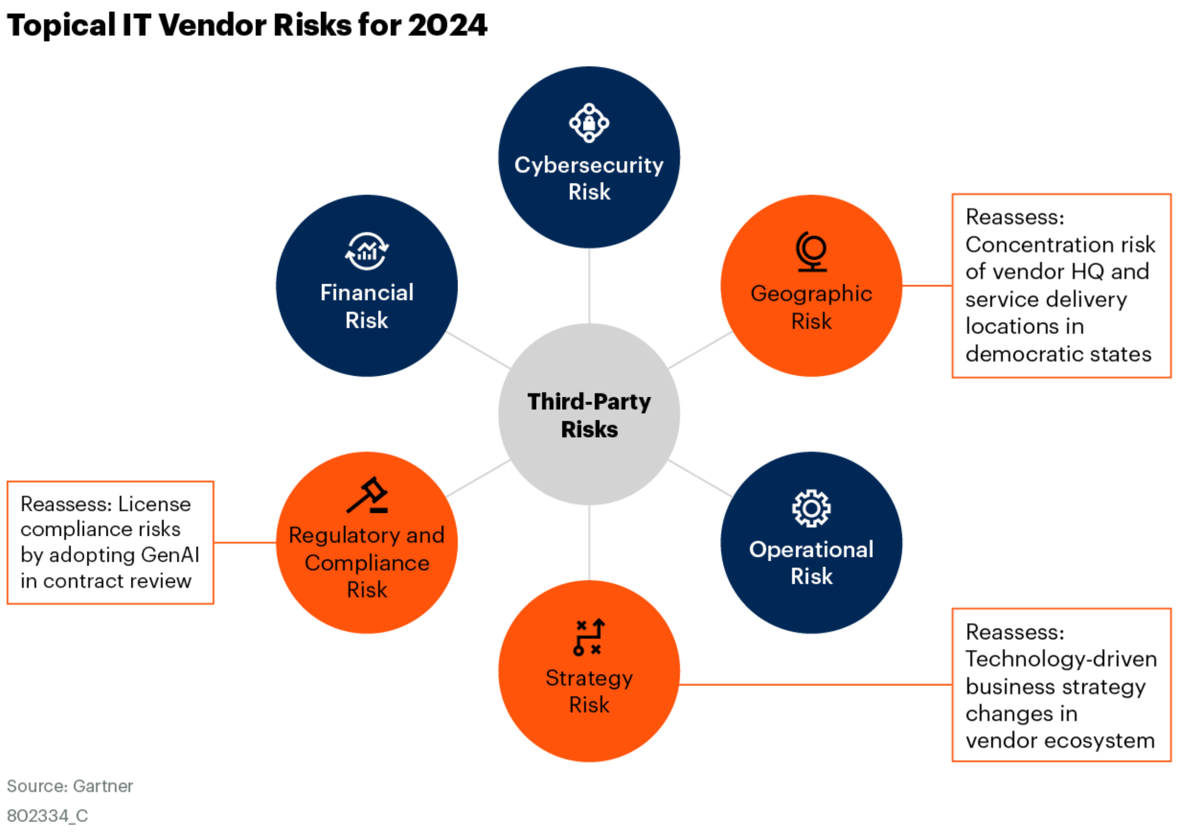
By 2028, generative AI's ability to decipher software and cloud vendor contracts will decrease the risk of noncompliance in software and cloud contracts by 30%.

Analysis

What You Need to Know

Geopolitical and technology-led disruptions necessitate a reassessment of the vendor risks across all risk categories, but sourcing, procurement, and vendor management (SPVM) leaders need to take new perspectives and approaches to reassessing and remediating geographic, strategy and operational risk categories (see Figure 1).

Figure 1: Topical IT Vendor Risks for 2024



Reassess: Concentration risk of vendor HQ and service delivery locations in democratic states

Reassess: License compliance risks by adopting GenAI in contract review

Reassess: Technology-driven business strategy changes in vendor ecosystem

Source: Gartner
802334_C

In addition to climate or natural disasters, currency fluctuations, legal, resource or infrastructure-related risks, the risk in terms of concentration of headquarters and service delivery locations of vendors in specific geographies is becoming a focus for organizations and regulators. For instance, the top 10 SaaS providers account for 50% of SaaS sales volume and have headquarters in the U.S and Europe, and the cloud infrastructure and platform services (CIPS) market is dominated by eight vendors accounting for 97% of the market with headquarters in the U.S and China. [1]

There are strategic risks associated with third-party support providers (TSPs), who have traditionally delivered software product support for enterprise software products like SAP and Oracle. With software providers pivoting to SaaS, third-party support providers are wary of losing their value proposition. TSPs are changing their business strategies by expanding their coverage to new products and delivering implementation and support services. SPVM leaders not only need to plan for such developments by preparing contingencies in case a vendor exits the market, but also take this opportunity to optimize their vendor portfolio by leveraging new offerings and swapping out poorly performing system integration vendors.

Regulatory and compliance risks can be addressed through the adoption of GenAI capabilities that can automate the assessment and monitoring of obligations in IT vendor contracts. Constantly evolving government and industry regulatory mandates, varying performance standards around cloud-based infrastructure and software, and growing complexity in licensing and subscription models is already driving digitization of contract management (see Market Guide for Advanced Contract Analytics).

> **Just as computer vision reinvented quality control in manufacturing production lines, generative AI will reinvent contract review.**

Leading contract life cycle management (CLM), enterprise legal management (ELM) and source to pay (S2P) providers are increasing their investments in generative AI and fortifying maturing use cases like automated contract review and contract risk analysis. This allows legal and contracting teams to quickly identify and address missing or noncompliant attributes. [2] SPVM leaders should embrace the new developments in GenAI and start pilots to improve productivity in high-volume contract reviews and reduce compliance risks.

Strategic Planning Assumptions

Strategic Planning Assumption: By 2027, geopolitical issues will increase the defaults in SaaS contract commitments, impacting over 50% of subscribers.

Analysis by: Tsuyoshi Ebina

Key Findings:

- According to Gartner's market share analysis, four of the top five SaaS vendors globally are headquartered in the U.S. Organizations across the globe are particularly dependent on U.S.-headquartered vendors for SaaS use. Economic sanctions can limit the ability to collaborate with service providers, and access restrictions can lead to severe service degradation. [1,3]

- During conflicts, SaaS providers' capacity to maintain data center loads is strained to the point where they are unable to deliver on promised service levels, such as uptime, performance and risk of service outages. [4]

- Major SaaS software vendors have significant development and delivery centers all over the world, including geopolitically sensitive areas (see Note 1), managed through a center of excellence model. For instance, security, product R&D, IT and customer support capabilities are typically sourced from locations like Russia, Israel, Eastern Europe, U.S., India and Southeast Asia. Service delivery degradation in one geography has a cascading effect on the overall contractual commitment.

- Organizations maintain an average of over 125 different SaaS applications totaling $1,040 per employee annually. IT typically is aware of only a third of those due to decentralized ownership and sourcing. Enterprises are increasingly becoming reliant on SaaS services so a service degradation presents high-risk exposure for organizations. [5]

Market Implications:

- In the near term, there may be an increase in the number of vendors who either cannot keep up their contractual commitments or may require a change to the contractual commitments. Examples of contractual commitment defaults include missed release cycles, product service levels (availability, reliability, usability), and support response times.

- SaaS is now used by all kinds of businesses in the enterprise. If the vendor's ability to deliver the committed service level deteriorates, the company's key businesses, including customer service, can find it difficult to continue doing business. Planned sales activities and product/service development may also be stalled due to SaaS service degradation.

- Additional business budget allocations will be required, to fund the switch from automated to manual work, or move workloads across data centers.

- Smaller organizations might face existential challenges, as derisking through redundancies or localizations may not be economically viable for them.

Recommendations:

- Require SaaS vendors to disclose the service delivery location of personnel involved in R&D, software development and support, not only for new contracts but also during contract renewals.
- Highlight the risks to business when negotiating contracts, and seek to mitigate the geopolitical risks by diversifying the hosting regions or zones.
- If a given location has higher geopolitical risk, take mitigating steps prior to signing the contract. Require the vendor to document the actions it will take in the event of an emergency and its impact to your organization.
- Update the business with the details provided by the vendor on potential risks, along with sourcing and procurement function's impact assessment, for its consideration and approval.
- Require vendors to contractually commit to notifying your organization of any changes in development or support locations for products or services in use.
- Check to see that appropriate service credits are in place for any reduction in the level of service. While the maximum amount of compensation is often capped at one year's subscription payment, negotiate for higher compensation if necessary. If the contract is multiyear, the maximum compensation should be at least the amount paid for the entire term of the contract.

- Consider the possibility that a SaaS vendor switch may be necessary as a last resort. Do not neglect to conduct regular research on alternative SaaS solutions that can be procured in each region. Confirm in advance the procedures to be followed when switching and the structure of the switching project.
- Incorporate geographic diversity as a key consideration for your business as it plans its future SaaS portfolio.

Related Research:

9 Geopolitical Implications of Generative AI

Prepare Your IT Vendor Contracts for the Risk of Disruption

Fundamental Elements of Business Continuity Management: Third-Party Risk and Contingency Management

Strategic Planning Assumption: By 2028, one of the main third-party support providers (TSP) will fail as software vendors successfully move customers to subscription-based models, creating potential vendor ecosystem risks for organizations.

Analysis by: Ciarán Hudson

Key Findings:

- Software vendors, including Oracle and SAP, continue to migrate customers to subscription models that include support, thus reducing or eliminating the need for third-party support. SAP's strategy is to increase its subscription revenue, and it expects up to 40% growth by 2025. [6]
- Software vendors often release new functionality on cloud-based versions that typically are offered on models before making it available on on-premises versions as part of their strategy to persuade customers to migrate to subscription.
- New capabilities and strategic innovations are increasingly only provided in subscription-based cloud solutions. SAP's latest strategic innovations, including generative AI and capabilities, will only be available in subscription-only cloud solutions. [7]

- Software vendors are increasing support costs for on-premises versions by between 4% and 8% annually, which makes subscription-based cloud offerings more compelling for customers. [8]

Market Implications:

- The potential market for third-party support will diminish in the medium term as software vendors migrate customers to subscription-based models that include support.

- There may be a short-term spike in customers choosing TSP to reduce annual support and maintenance costs, before deciding on the next stage of their ERP journey.

- TSP providers will have to expand their services beyond their traditional offering in order to survive. Rimini Street has launched its Rimini ONE offering, which includes services beyond TPS.

- TSP providers will struggle to attract and retain staff with the required expertise in a diminishing market.

Recommendations:

- Customers with TSP should perform a risk analysis to assess the impact should their TSP provider fail. The risk assessment should include impact to operational activities, services that can be provided internally, alternative providers, the cost of returning to vendor support and any back maintenance that will be due.

- Risk management of TSP’s liquidity and solvency should be performed periodically.

- Escrow arrangements should be placed to be used in the event of any TSP failure. The escrow agreement should guarantee access to software source code in the event of market exit.

- If the TSP is a publicly traded company, review its income statements over the last four quarters to understand how expenses have changed in relation to revenue. If the ratios have not changed significantly, leverage that information to push back on increases.

Strategic Planning Assumption: By 2028, generative AI's ability to decipher software and cloud vendor contracts will decrease the risk of noncompliance in software and cloud contracts by 30%.

Analysis by: Ben Jepson and Yoann Bianic

Key Findings:

- Software and cloud vendors' terms and conditions (T&Cs) and use rights within IT contracts are complex, ever-changing, and often in multiple documents. This makes them very hard to interpret and decipher, increasing the risk of noncompliance and exposing organizations to legal issues.

- It is the customer's responsibility to remain compliant with vendor contract T&Cs. This requires SPVM leaders to spend considerable amounts of time manually reading and analyzing large volumes of content within IT contracts and identifying areas that carry license compliance risk that could expose their organization.

- From an ongoing license management perspective, if business requirements, consumption or T&Cs change, SPVM leaders will have to evaluate the impacts and act accordingly on both the procurement and technical sides. GenAI could help to automate the assessment of opportunities and risk when there are changes, either on the demand side (consumption of software) or offer side (entitlements, use rights, licenses).

- GenAI can simplify the way SPVM leaders access and interpret software and cloud vendors' T&Cs by taking advantage of natural language processing (NLP). This technology could even be trained or fine-tuned to integrate specific, customized contractual language, as well as elements of consumption, to enable a more robust IT contract.

Market Implications:

- GenAI will be used to manage software and cloud contracts as integrated in SAM/IT asset management tools, contract management tools, or mainstream GenAI tools. It will enable analysis of standard contract T&Cs, but also of customized and negotiated terms, to reflect an organization's actual situation. For example, GenAI must be able to analyze amended metrics, BYOL rights or deployment rights. Otherwise, outputs could be misleading and inaccurate.

- Compliance is the balance between entitlements (contained in contracts) and consumption. GenAI's ability to calculate an organization's exposure based on its actual versus contracted consumption of software will enable SPVM leaders to make quick, informed and balanced licensing decisions.

- SAM functions within organizations will use GenAI to automate the licensing desk process for its business users, asking questions about the use rights and limitations of the products they deploy and manage. This will help to streamline license management processes.

- SAM teams will use GenAI to make better use of SAM tools, by adding an NLP layer enabling easier access to certain effective license positions, upcoming renewals, and risky situations. It will free up time for SPVM leaders and enable them to focus on optimization exercises to identify more cost-effective ways of licensing their products and ultimately save on license costs.

Recommendations:

- SPVM leaders and SAM teams must maintain accurate and updated contract and procurement data, including documents that are not publicly available (such as negotiated or confidential addendums). This will allow GenAI to capture the full picture regarding an organization's entitlement.

- SPVM leaders must carefully test GenAI tools and then design and train those against their own context and consumption, to go beyond just use rights and have visibility over their effective license position. SPVM leaders must also ensure that the results are accurate, verifiable and reliable.

- There are privacy implications with regard to training the GenAI models. SPVM leaders need to get assurances from vendors that their organization's data isn't used to train a general-purpose large language model (LLM) of the vendor. If a vendor is unable to provide appropriate assurance, SPVM leaders need to consider private LLMs as an alternative.

- SPVM leaders should evaluate the use of GenAI in order to automate the licensing desk layers of their SAM function. Examples include daily questions about licensing rules, limitations, and impacts of architecture changes.

- SPVM leaders and SAM teams should use the time saved from implementing GenAI into their internal SAM function to concentrate on license optimization exercises. Assess usage of vendor products and analyze different licensing options and competitive alternatives in an effort to optimize overall software license costs.

Related Research:

Quick Answer: How Can I Address Generative AI Risk in IT Contracts?

The Future of the Software Asset Manager Is About Governance, Not Counting Licenses

Target Software and Cloud Costs by Uniting Software Asset Management and FinOps

A Look Back

In response to your requests, we are taking a look back at some key predictions from previous years. We have intentionally selected predictions from opposite ends of the scale — one where we were wholly or largely on target, as well as one we missed.

This report is too new to have on-target or missed predictions.

Evidence

[1] Market Share: Enterprise Public Cloud Services, Worldwide, 2022.

[2] Market announcements by iCertis and Docusign: Icertis Brings Generative AI to Enterprise Contracting With Delivery of First Contract Intelligence Copilots, Icertis; DocuSign Piloting Future of Smart Agreements With Google Cloud's Vertex AI, DocuSign.

[3] U.S. Government Blacklists China's Largest Server Maker Inspur, Used by Cisco, IBM, Intel, NVIDIA, Data Centre Dynamics.

[4] Russian-Ukraine Armed Conflict: Lessons Learned on the Digital Ecosystem, ScienceDirect.

[5] Market Guide for SaaS Management Platforms.

[6] SAP Investor Relations Outlook, 2023, SAP.

[7] SAP SE (SAP) Q2 2023 Earnings Call Transcript, Seeking Alpha.

[8] Price increases by software and SaaS vendors: see What Do Salesforce's 2023 Price Increases Mean for Customers? and Quick Answer: What Actions Can Minimize the Impact of Microsoft's Regional Pricing Increases?.

Note 1: Geopolitical Risk

Geopolitical risk refers to the risk that heightened political or economic tensions in a particular country or region will threaten other regions or the world. The Eurasian coastal region from northeastern China through Southeast Asia, the Indian peninsula, the Middle East, and continental Europe, commonly referred to as the "Rimland," is the major geopolitical area where heightened tensions are more likely to occur than other areas.

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

IT Vendor Ecosystems Management Primer for 2023

Innovation Insight for Generative AI

Formalize Vendor Risk Management to Reduce Business Disruption

Fundamental Elements of Business Continuity Management — Governance and Program Management