



# The Future of Trust

The Evolving  
Threat Landscape

January 2021

---

Select the right professional services firm  
— one with the industry depth, knowledge,  
and insight to help clients address their  
most pressing issues.

[kpmg.com](https://kpmg.com)

# The evolving threat landscape

**No threat is more dangerous than the one lurking inside of an organization**—a fact too often made painfully clear to government officials and private sector leaders. Federal agencies are faced with increasingly high-profile incidents of classified information leaks, intellectual property theft, fraud, and exploitation by foreign adversaries. Agencies are under intense pressure to identify and mitigate a full range of risks within their workforce and supplier network, commercial off-the-shelf (COTS) products, and the supply chain. In order to counter the expanding volume of threats, agencies need to make trust determinations around the most critical entry points: the people, entities, and products that impact the mission.



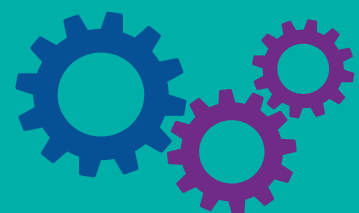
Understanding the **right data sets to proactively predict, identify, and mitigate risks to critical assets** is essential. However, operationalizing this data can seem impossible in an environment characterized by too much uncertainty and competing risk management priorities. Today's fastevolving threat environment requires not just a proactive solution but one that is also comprehensive.

## KPMG's approach

KPMG's Future of Trust solution is the first and only proactive, holistic solution designed specifically to help federal agencies identify the full spectrum of risks within their workforce, third-party suppliers, COTS hardware, and software. This singular approach provides overlap across risk areas and helps ensure a much safer environment. **The Future of Trust** includes a mission-centric, tailored methodology to **reduce complexity, provide new insights, and drive threat-based decisionmaking. Our clients are able to reduce risk by increasing trust and reliance** in people, products, and entities.

Informed by KPMG's deep subject matter knowledge in data science, forensics, behavioral psychology, counterintelligence, and threat trends, the Future of Trust solution provides a leading view of the threat landscape, security, and regulatory requirements to help clients make timely, reliable, data-driven trust determinations.

## Trusted relationship stages

	Onboarding	Continuous evaluation	Offboarding
 People	Rapid automated background investigations	Automated risk flagging Behavioral and technical risk indicators	Access control removal Preseparation activity monitoring
 Entities	Commercially enabled due diligence Foreign ownership, control, & influence assessment	Viability risk monitoring Comprehensive supply chain mapping	Offboard when risk thresholds are met Identify alternate lowerrisk suppliers
 Products	Provenance risk assessment Counterfeit probability assessment	Integrity risk assessment Quality risk assessment	Identify lower-risk alternative parts

# How we can help with trust determinations

**Making an initial determination is just that: initial.**

## Trusted personnel

Personnel risk can be a serious threat vector to an agency in the form of both outsiders and insiders. Making the right initial trust determination when allowing new personnel access into an agency is critical. Additionally, once the initial trust determination has been made, continuous evaluation of behavioral and technical indicators is vital to ensure that the person continues to act in a trustworthy matter. KPMG is actively working with federal policymakers and our clients to engage our leading commercial capabilities in advanced data and analytics, machine learning, and artificial intelligence to develop solutions that won't introduce additional risk into the process. Incorporating better data management and advanced analytics can provide significant advantages in personnel trust determinations.



**AI enables agencies to assess risk in people, entities, and products**

**Driven by comprehensive proprietary data sets**

## Establishing a network of trusted entities

Third-party risk management and business intelligence are valuable tools for discovering risk in an organization's supply chain. Our proprietary diligence and intelligence solutions coupled with our unique access to private company data provide transparency into the following areas of supply chain security: insight into hidden relationships, cyber threats, insider threats, counterfeit parts, and risk from foreign ownership, control, and influence (FOCI) concerns that may affect an organization through its network of vendors and suppliers. Tracking, managing, and appropriately reacting to that information requires tact, a solid case, and business management capability.



## Evaluating technology for compromise

Even when technology is acquired from a trusted vendor, it may still be subject to the threat of compromise, counterfeit components, or product substitution. KPMG employs an advanced data and analytics capability and proprietary data sets to assess the quality, integrity, and provenance of all microelectronic components in any commercial off-the-shelf hardware. This approach is used to identify counterfeit or compromised parts, identify the point of origin and third-party risk for each component, and assess overall risk associated with a specific component either before or after it has been acquired.

# Use cases and past experience

## **Critical technology protection –**

KPMG conducted forensic Integrity Due Diligence research on supply chain risk concerns for a U.S. agency's global acquisition office. Our cleared analytic team conducted both OSINT and classified research to provide actionable intelligence assessments to the defense acquisition community through mapping the supply chain and third-party networks, identifying FOCI concerns, and highlighting derogatory or suspicious financial behavior.

## **Fraud risk management –**

KPMG conducted risk assessments for a government agency on over 80 third-parties to aid in quantifying reputational and legal risk factors for grant recipients, specifically public housing authorities and municipalities. Moderate-to-high risk findings illuminated misuse of taxpayer funds, fraud, corruption and bribery, financial viability, noncompliance with federal law and regulation, subpar performance, and health and safety issues.

## **Personnel vetting –**

KPMG created an OSINT risk engine for a major DoD entity to assist with personnel security investigations based on behavioral psychology, insider threat best practices, legal data, and other commercially available sources to generate insights into personnel risk to drive decision-making.

## **Financial intelligence –**

KPMG leveraged leading commercial due diligence, financial and banking experience, and capabilities for a government agency to drive modernization of risk management strategy, methodologies, and technology. KPMG leveraged a combined proprietary solution, including a financial transaction monitor tool used in the banking sector, and other capabilities to assist the client's analytic team with Know Your Customer (KYC) due diligence and risk assessment reviews for potential vendors and private sector partners.

## **Hardware provenance –**

A defense research laboratory sponsored a challenge for KPMG to quickly and reliably assess quality, integrity, provenance, and risk of any commercial off-the-shelf hardware. KPMG's solution reliably identified the point of design and manufacture, as well as hidden vulnerabilities, FOCI concerns, and other counterintelligence risk factors that were previously unknown to the client.



**Architected by career intelligence officers**



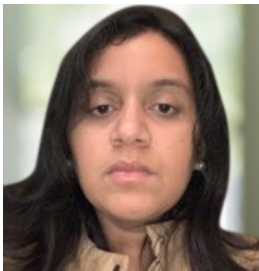
**David Buckley**  
**Managing Director, FED Forensic**  
**C:** 703-286-8489  
**E:** davidbuckley@kpmg.com



**Viral Chawda**  
**Principal, FED Digital Lighthouse**  
**C:** 832-535-8712  
**E:** vchawda@kpmg.com



**Fred Gortler**  
**Director, FED Forensic**  
**C:** 703-883-7925  
**E:** fgortler@kpmg.com



**Uma Radhakrishnan**  
**Managing Director, Tax Economic & Valuation Services**  
**C:** 516-312-8724  
**E:** uradhakrishnan@kpmg.com



**Michael Artiglio**  
**Director, FED Forensic**  
**C:** 571-814-0691  
**E:** martiglio@kpmg.com



**Arun Aggarwal**  
**Specialist Director, FED Digital Lighthouse**  
**C:** 816-645-3168  
**E:** arunaggarwal@kpmg.com



**Challen Parker**  
**Director, FED Digital Lighthouse**  
**C:** 703-307-4193  
**E:** challenparker@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

[kpmg.com/socialmedia](https://kpmg.com/socialmedia)



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2021 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. NDP153703

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.