

# Managing CFIUS Compliance: Four Pillars for Success

## CFIUS Compliance Begins Before the Deal is Signed

Outside of Washington, D.C., the Committee on Foreign Investment in the United States (CFIUS or the Committee) was once called “the most powerful government organization you’ve never heard of.” Against a backdrop of shifting global trade dynamics, technological competition, and concerns with foreign investment, that perception of CFIUS has morphed into what a New York Times’ story called “the ultimate regulatory bazooka.” With the expanded authority of CFIUS under the Foreign Investment Risk Review Modernization Act (FIRRMA)<sup>2</sup> now fully implemented in regulation, new types of deals are in the cross hairs. Many businesses are asking for the first time, “How do I establish a CFIUS program that facilitates the success of my transaction and my business?” Doing so can be a significant undertaking, but Kroll recommends four simple, first steps to take.



## Prepare

### Assess Your Own CFIUS Risk

Successful CFIUS compliance begins before preparing a notice for the Committee. The essence of good CFIUS preparation is developing a clear understanding of your transaction in a CFIUS context. U.S. targets and foreign investors need to understand how CFIUS will view their transactions by conducting thorough due diligence. That due diligence should include, for example, understanding the foreign investor's ties to foreign governments and its history of complying with U.S. laws and regulations. Transaction parties must also understand what aspects of the target business CFIUS is likely to see as vulnerable to exploitation from a national security perspective. Moreover, parties to elevated-risk transactions should determine what forms of national security risk mitigation would be acceptable and consider proposing those mitigations to CFIUS.

Preparation also includes establishing a robust understanding of baseline security controls for the business, covering both physical security and cyber security. This baseline will be the foundation for any new controls that implement CFIUS-mandated mitigation. Without it, parties are often poorly equipped to negotiate CFIUS mitigation agreements and risk incurring obligations that they cannot implement. Well-prepared parties, however, can negotiate mitigation terms knowing what new controls can be practically implemented as well as the timeframe and costs related to that implementation.

## Organize

### Design and Implement a Robust and Operational CFIUS Compliance Program

Well-executed organization is another simple, yet critical pillar of a successful CFIUS compliance program. For a smooth CFIUS review, parties should select experienced CFIUS counsel who can track the numerous information requests and tight timelines for responses.

At the conclusion of the review, should CFIUS mitigate your transaction, a well-organized compliance program becomes a necessity almost overnight. Busy compliance and security officers need a prioritized implementation plan marking the critical path to expeditious and full compliance. While typical mitigation agreements

prescribe a series of near-term deadlines that are important markers, they do not always tell the full story. Achieving more distant agreement milestones may necessitate precursor activities that must be taken immediately. As an example, an annual report due in 12 months may require a review of visitor logs. To achieve compliance, however, the security team must begin collecting and preserving visitor logs immediately. Backward planning from the due date of the first annual report can be an effective method for staying organized and managing the complexity of CFIUS compliance programs.

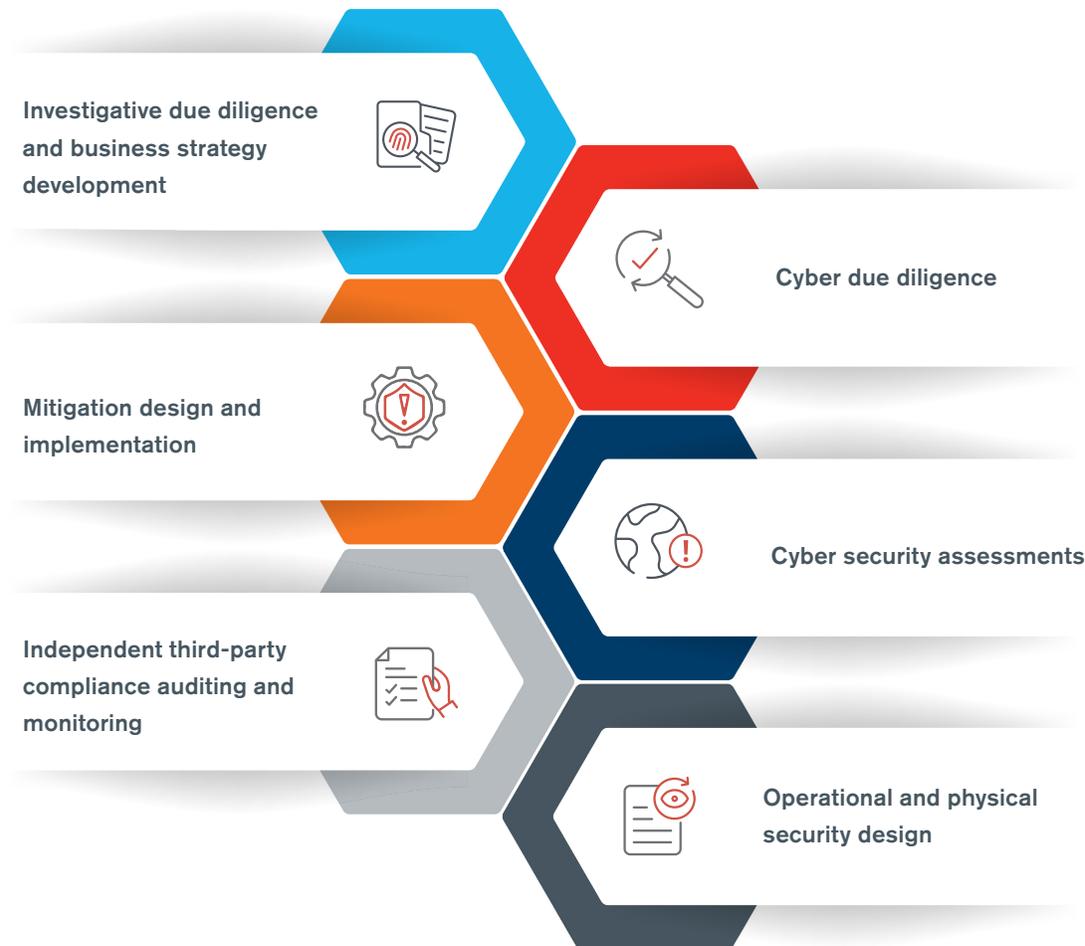
## Communicate

### Establish Open Communication Channels to Support Your CFIUS Compliance Program

Frequent, open communication about your CFIUS compliance program establishes expectations at all levels of your business and creates the relationships that enable the business to weather unexpected contingencies. Communication should begin with the most senior members of the company, including the board of directors and CEO. Without authentic leadership support, even the most diligent security officer faces an uphill battle operating an effective CFIUS compliance program. In addition to managing upward to senior leadership, CFIUS compliance teams need to send clear, top-down communications that broadly share the compliance expectations with company staff. For staff working in particularly sensitive areas, these communication efforts may even warrant an annual certification program affirming staff awareness and understanding.

Mitigated parties should also actively communicate with the CFIUS monitoring agencies. Entering into a CFIUS mitigation agreement is similar to entering any other long-term relationship—communication increases confidence and creates strength in the face of adversity. Despite upfront planning, security officers sometimes discover previously unrevealed issues that may affect compliance with the agreement. In those circumstances, expeditious communication with the CFIUS monitoring agency, including a remediation plan with frequent milestones, could be the difference between success and failure.

## Kroll CFIUS and National Security Services



## Engage

### Engage Experienced CFIUS Advisors

For some companies, the CFIUS process is their first direct encounter with the national security apparatus of the United States. Failure to anticipate the likely scenarios arising in a CFIUS review or to comply with mitigation obligations can be costly. As an example, in the spring of 2019, CFIUS fined an unidentified company USD 1 million for failure to comply with its mitigation obligations. Instead of going at it alone, parties to foreign investment transactions should engage expert assistance, in the form of experienced CFIUS counsel and risk solutions firms like Kroll.

#### Citations:

1. <https://www.nytimes.com/2018/03/05/business/what-is-cfius.html>,
2. [https://home.treasury.gov/sites/default/files/2018-08/The-Foreign-Investment-Risk-Review-Modernization-Act-of-2018-FIRRMA\\_0.pdf](https://home.treasury.gov/sites/default/files/2018-08/The-Foreign-Investment-Risk-Review-Modernization-Act-of-2018-FIRRMA_0.pdf).

For more resources and insights visit:  
[Kroll.com/cfius](https://kroll.com/cfius)

## AUTHORS



**Samuel P. Jacobs**  
Associate Managing Director  
Cyber Risk  
+1 202 649 1264  
[samuel.jacobs@kroll.com](mailto:samuel.jacobs@kroll.com)



**Nicole Lamb-Hale**  
Managing Director  
Business Intelligence and Investigations  
+1 202 450 0318  
[nicole.lamb-hale@kroll.com](mailto:nicole.lamb-hale@kroll.com)

---

## TALK TO A KROLL EXPERT TODAY

**North America**  
T: 877.300.6816

**UK**  
T: 08081012168

**Australia**  
T: 1800870399

**Hong Kong**  
T: 800908015

**Singapore**  
T: 8001013633

Or via email: [cfius@kroll.com](mailto:cfius@kroll.com)

[kroll.com/cfius](https://kroll.com/cfius)

---

**About Kroll** Kroll is the leading global provider of risk solutions. For more than 45 years, Kroll has helped clients make confident risk management decisions about people, assets, operations and security through a wide range of investigations, cyber security, due diligence and compliance, physical and operational security and data and information management services. For more information, visit [www.kroll.com](https://www.kroll.com).

**About Duff & Phelps** Kroll is a division of Duff & Phelps, a global advisor with nearly 4,000 professionals in 25 countries around the world. Our clients include publicly traded and privately held companies, law firms, government entities and investment organizations such as private equity firms and hedge funds. We also advise the world's leading standard-setting bodies on valuation and governance best practices. For more information, visit [www.duffandphelps.com](https://www.duffandphelps.com).