Building a better working world

Optimize your organization's high-value asset identification capability

Understanding and managing high-value assets (HVA) has become an essential component of senior management and business process owners' risk management program. The ability to identify and protect HVA plays a critical role across the organization in allocating resources to provide the greatest protection and resiliency to the data, processes and systems that matter most to the organization.

A modified version of this article appeared in Global Association of Risk Professional (GARP) Risk Intelligence.

High-value assets (HVA) are more than just your most valuable line items on the balance sheet. Beyond their monetary value, organizations need to consider the enterprise-wide impact HVAs have on cross-functional processes such as operations, compliance and legal as well as on broader risks (including reputational risk, liquidity and resiliency.)

For example, a bank's enterprise risk management (ERM) system containing 200 records may be valued on the balance sheet at just US$50,000. Yet if that ERM system were unavailable during the trading day, it would halt the business in its tracks. Moreover, if the contents were stolen or altered, the bank would suffer severe reputational damage. These financial, legal and reputational risks are leading organizations to take a differentiated approach to asset protection that places appropriate controls on HVA broadly defined.

HVA includes any elements of critical business processes, applications, data and infrastructure that must be protected to provide for the continued confidentiality, availability and integrity (CIA) of information. *Confidentiality* refers to systems that store and process sensitive data that must be protected to maintain an organization's reputation, achieve compliance with laws and regulations, and protect intellectual property or trade secrets. *Availability* refers to systems needed to maintain an organization's continued operations and ability to execute in the market. *Integrity* refers to the systems and processes that help ensure that data and information within the ecosystem is complete and accurate.

Regulators are starting to include HVA identification as part of their mandated risk assessments. For example, in October 2016, banking regulators published an Advanced Notice of Proposed Rulemaking (ANPR) on enhanced cyber risk management.[1] The ANPR calls for board-level responsibility over financial ecosystem resiliency, including identification of system-critical assets to prevent the failure of a single organization from taking down the rest of the ecosystem.

Also, earlier this year, New York State Department of Financial Services put into effect new cybersecurity requirements for financial services companies,[2] including requirements for written policies and periodic risk assessments throughout operations. Similar risk-assessment regulations can be found in other financial capitals, whether from European Union regulators, the Bank of England, or the Monetary Authority of Singapore, and we expect the trend toward regulated risk assessments to continue in other global markets.

The international regulatory pressure for better HVA management is being driven by two main factors: first, cyber attackers have put financial institutions in their crosshairs, making it even more important for firms to identify their own weak spots ahead of their adversaries; and second, financial institutions have introduced new potential risks based on changes to their business models.

Having a comprehensive understanding of HVA enables an organization to:

- Align critical business processes, applications, data, and infrastructure
- Prioritize and enhance defenses against cyber attacks
- Develop a tailored backup and resiliency strategy
- Meet board and market expectations
- Respond quickly to market conditions
- Assist with regulatory risk assessments and expectations

Yet despite the importance of understanding HVA, most organizations lack a formal process to identify HVA, and have limited ability to understand the upstream/downstream data flows and dependencies within the business.

[1] EY, Advance Notice of Proposed Rulemaking (ANPR) or Enhanced cyber risk management standards for financial institutions, January 2017.

[2] EY, Cybersecurity requirements for financial services companies: Overview of the finalized Cybersecurity Requirements from the New York State Department of Financial Services (DFS), February 2017.

HVA driver #1: increased risk posed by cyber attackers

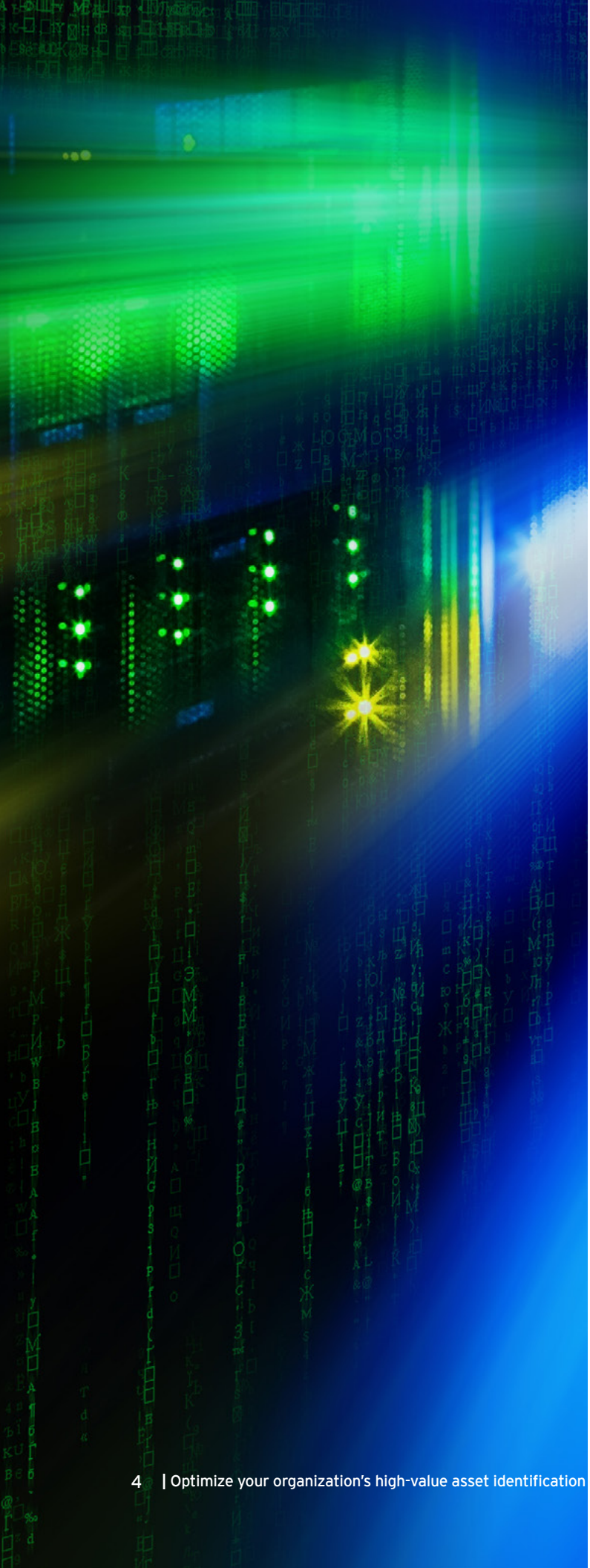
The first driver of the push toward better HVA management is the ceaseless probing by cyber attackers seeking weak points. Financial institutions, especially those considered to be critical infrastructure such as clearing networks and stock exchanges, are under constant threat from cyber attackers of all types, from hacktivists to hostile nation-states. Financial institutions also must cope with increasingly sophisticated attacks by adversaries with a profit motive, whether it's attackers stealing and reselling customer data, or committing financial crimes, and then covering their digital tracks. For any of these attackers, finding a financial institution's unguarded HVA poses a serious threat. If an entire business process relies upon a component, even if it is a relatively small subsystem, that component should be considered as part of HVA and protected to an appropriate extent.

Moreover, it's not just about protection, as even the best-prepared organizations can get hit with an attack. As part of the response to increasingly virulent cyber attackers, financial institutions need to increase the speed and flexibility of their approaches to operational restoration. Following 9/11, many within the financial services industry worked to enhance their recovery capabilities by focusing on the "critical flow" required to restore a minimum level of service within days. The typical approach to Disaster Recovery, Business Continuity and Backup/Retention relies upon replicating a snapshot of enterprise data at a single point in time.

In today's world, organizations need a holistic resiliency strategy that focuses on all HVAs and restores full service on a much faster timetable; the "snapshot" approach is far too slow. For some HVAs, even hours of downtime, particularly depending on the time of the day or week or month, would pose a serious problem.

For example, if your customer information file has been encrypted by ransomware, you'll need to roll-back and roll-forward selected data elements in a carefully staged manner, and that's extremely difficult to choreograph for organizations that only deal with enterprise-wide snapshots. In a recent cyberattack, one organization took three days to recover because they couldn't distinguish the high-value data they needed to restore operations from the less-critical data that could wait until later.

The clear need in this situation is to have a structured process to identify HVA independently of the broader snapshot of full enterprise data. Suppose you're trying to recover from a ransomware attack on critical system resources. Unless you know precisely which assets need to be deployed, and in which order, to restore operations at a minimum viable level, you're not prepared for the current threat environment.



HVA driver #2: faster pace of deployment from new business models

Technology disruptors like digital delivery continues to change business models for financial institutions. To embrace digital delivery, financial institutions are constantly being pressured to move quickly with new initiatives, new applications and new products. This creates a natural tension with the operational constraints of maintaining integrity, resiliency, privacy and security.

Yet financial institutions' "Do no harm" approach to protecting the customer has limited the pace of change, and this has turned out to be a competitive liability for large financial institutions versus Fintech companies. Unlike traditional financial services firms subject to a high level of oversight and expectations, Fintech companies tend to move quickly with a "fast-to-fail" strategy, in which they deploy into the market products that are only 80% to 90% ready and then adjust accordingly. This approach is difficult for financial services firms to imitate, both because of their internal culture and expectations to protect the marketplace and consumers.

As one approach to speeding up delivery times, financial institutions are exploring new development methodologies that enable rapid prototyping and fast deployment, modifying traditional checkpoints in the development cycle. While these methodologies bring new products to market more quickly, it compresses the time available for organizations to ensure that they have met all relevant expectations regarding continued operations, market expectations, privacy, and reputation. Furthermore, digitized processes often lack manual fallbacks given reduced headcount, which increases the reliance on resilient architectures and recovery strategies. Given the compressed timeframe and heightened need for resilience, these new development methodologies must be backed by assurances that HVA along with all HVA-dependent assets have been fully considered prior to launch.

What's missing in the current approach to HVA

Most firms lack a formal, enterprise-scoped process to identify HVA, relying instead on ad-hoc approaches managed by separate business units.

The ad-hoc approach overlooks critical HVA and fails to identify dependencies between assets. This leads to overinvesting in less-important items, and underinvesting in more-important items.

Each business unit tends to measure operational risk in its own way, and in doing so, protects its own budgets, systems and processes. Businesses tend to prioritize their own systems, and that happens even when the baseline functioning of the organization relies more heavily upon processes of other business units.

Moreover, higher-revenue departments tend to have better protection for their data and processes, even if other functions are more critical to the overall operation of the firm. For example, if you're trading desk gets shut down for a day, that's bad. But if your Settlement & Clearing team can't settle trades already on the books, that's worse – both in terms of reputation and liquidity. Nevertheless, it's a good bet that the typical revenue-center trading team gets better technology support than a cost-center risk management team. Front-office systems may be given higher priority than middle-office risk management, even though some of the operations or risk management functions would need to be operating immediately following a crisis.

To counteract these tendencies, firms will need to compile a comprehensive enterprise view of business processes, applications, data and infrastructure, uncovering interdependencies between businesses and identifying the HVAs that are essential to preserving the value of the entire enterprise, regardless of business unit responsibilities. These interdependencies affect resiliency planning, backup strategies, privacy, security, reputation and regulatory expectations.

For example:

- Customer service agents often rely upon a consolidated view of the customer across multiple departments. If restoring functionality to your business depends on customer service agents, before you go back online after an outage, you need that consolidated view to work; and in turn, all the processes that feed into the consolidated view must also work.
- If you're a consumer lender that supports a wide range of products with external consumer credit ratings, do you know what the implications would be if you had any connectivity problems with that vendor? How long would it take for you to restore functionality to your loan origination processes?
- Wire transfers enable you to settle with your counterparties, which is essential for credit and market liquidity. Yet the wire transfer system may not be at the top of enterprise's list within the business units that use the capability.

In each of these examples, it's unclear for companies to determine how to prioritize, and who should prioritize, the shared resource used by multiple divisions.

How to establish ongoing processes for high-value asset identification

The most difficult part of high-value asset identification won't be the mechanics of identifying HVA, managing an HVA initiative or even paying for it. Instead, the hardest part is challenging the proprietary sense of ownership held by individual business units regarding their own applications. In other words, people tend to protect their own turf. If you tell someone that their department's applications no longer take precedence during a business operation, there will be pushback. It's also a fairly sure truth that you'll hear about it when budgets get moved around to match the criticality of HVA from an enterprise standpoint.

That's why we recommend that you proceed with a combined "top-down" and "bottom-up" approach to HVA, which provides the necessary combination of institutional backing and on-the-ground detail to earn the backing, understanding and acceptance of the stakeholders involved. This combined approach resembles similar exercises that firms have taken in other contexts, such as with recovery and resolution plans (RRP).

"Top-down" identifies the most important HVAs by drawing upon an enterprise-wide view of an organization. With this approach, you should review the enterprise profile from business process, systems, server and data standpoints, working through the assets being protected and backed up.

"Bottom-up" recursively scans the enterprise through each business unit and department, tracing data flows and process flows to identify dependencies.

With data gathered through both approaches, you can then create holistic risk profiles of assets, measured in terms of business criticality. Based on that information, you can decide what to prioritize at the enterprise level, and then validate those priorities against existing risk management frameworks.

HVA identification is an ongoing process that changes as your business changes, not a one-time initiative resulting in a report to be filed away on a server. For example, if you become active in M&A, you may need to treat otherwise ordinary business data as HVA to be protected from inadvertent disclosure or data breach that could jeopardize a deal. Given the wide scope of activities performed by any large-scale organization, HVA identification needs to provide real-time visibility over the "crown jewels" of the enterprise.

The hardest part of HVA is challenging the proprietary sense of ownership held by individual business units regarding their own applications.

"Top-down" approach identifies the most important high-value assets by drawing upon an enterprise view of an organization.

"Bottom-up" recursively scans the enterprise through each business unit and department, tracing data flows and process flows to identify dependencies.

The HVA-optimized enterprise

With HVA identification in place, your enterprise can:

- Focus on what matters most. Put your limited budgets where they're most needed, protecting the most sensitive assets from compromise.
- Improve organizational views of operational risk management, at high levels of efficiency and effectiveness.
- Maintain the integrity of business functions under adverse operating conditions.
- Bolster resilience following a physical or cyber attack by preparing to take the fastest and most efficient path to viable operations.
- Meet new regulatory mandates with comprehensive risk assessments backed by a robust methodology.
- Race ahead with new digital initiatives with the confidence that HVAs are under constant observation by a dedicated team.

Most importantly, organizations that gain experience managing HVA as an ongoing process will become better at maintaining proactive defenses in the face of ever-changing threats. Once you find that employees, on their own initiative, start to point out potential HVAs that need to be defended at an enterprise level, you'll know that you've achieved a valuable shift in thinking that will better prepare your organization well for the future.

EY contacts

Tom Campanile
+1 212 773 8461
thomas.campanile@ey.com

Cindy Doe
+1 617 375 4558
cynthia.doe@ey.com

John Doherty
+1 212 773 2734
john.doherty@ey.com

Sundeep Nehra
+1 212 773 3888
sundeep.nehra@ey.com

Tim Purtell
+1 212 773 1232
tim.purtell@ey.com

Roy Thetford
+1 212 773 3951
roy.thetford@ey.com

Mark Watson
+1 617 305 2217
mark.watson@ey.com

Chip Wentz
+1 919 981 2861
chip.wentz@ey.com

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

EY is a leader in serving the global financial services marketplace
Nearly 51,000 EY financial services professionals around the world provide integrated assurance, tax, transaction and advisory services to our asset management, banking, capital markets and insurance clients. In the Americas, EY is the only public accounting organization with a separate business unit dedicated to the financial services marketplace. Created in 2000, the Americas Financial Services Organization today includes more than 11,000 professionals at member firms in over 50 locations throughout the US, the Caribbean and Latin America.

EY professionals in our financial services practices worldwide align with key global industry groups, including EY's Global Wealth & Asset Management Center, Global Banking & Capital Markets Center, Global Insurance Center and Global Private Equity Center, which act as hubs for sharing industry-focused knowledge on current and emerging trends and regulations in order to help our clients address key issues. Our practitioners span many disciplines and provide a well-rounded understanding of business issues and challenges, as well as integrated services to our clients.

With a global presence and industry-focused advice, EY's financial services professionals provide high-quality assurance, tax, transaction and advisory services, including operations, process improvement, risk and technology, to financial services companies worldwide.

EYG no. 000000
1707-2358371 BDFSO
ED None

ey.com