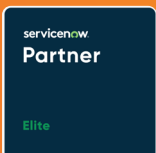




For ServiceNow® users

A new way for business owners to manage risk





In this guide, you'll learn:



Why traditional risk approaches aren't right for every business



What high-value functions are and why they're important



How to grow and manage risk at the same time



The five steps to rolling out a high-value function risk approach





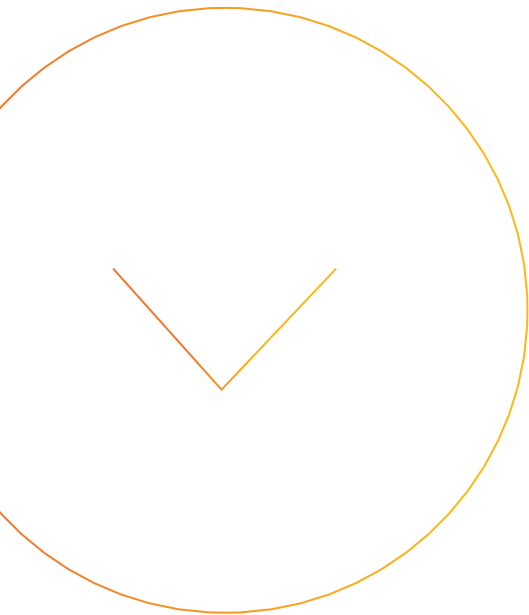
Are you tired of constantly worrying about whether your business is safe from risk?

All too often, companies invest countless hours and finances into implementing risk management programs that still don't help them reach their desired level of maturity. **The truth is that traditional risk approaches don't work for every business.**

For some businesses, traditional risk management results in analysis paralysis. These organizations require a more flexible, efficient approach that allows them to focus on what matters most without being weighed down by complexity.

Allow us to introduce our high-value function approach to risk management. 





What is a high-value function?

A high-value function is a collection of interdependent entities – including processes, applications, vendors, and more – that could have negative impacts on an organization’s cash flow, reputation, and overall business growth if compromised.

Once high-value functions are identified, each function and its dependencies are onboarded into the integrated risk management (IRM) program. Essentially, this creates a full IRM program for each function by mapping its risks, controls, vendors, and business continuity plans. The final step is getting to an automated state for continuous monitoring and testing without manual intervention.





Why opt for a high-value function approach?

Traditional approaches to risk management often are shortsighted, focusing more on tools and technology than on value and action. They can require months – if not years – to fully implement, which drains time and budgets while leaving critical assets unsecured.

Here are just a few of the areas where traditional risk approaches fall short:

- Too many technologies
- Lack of resources
- Incomplete risk and control frameworks
- Inaccurate organizational structures
- Incomplete process and asset inventories
- Changing business objectives

So how is a high-value function approach different?

In short, **organizations can grow and manage risk at the same time** because they have a clear understanding of what's most important to the business from the outset.

With a high-value function approach, businesses can implement a top-to-bottom, integrated risk program because they're focusing on one key business function at a time. This way, organizations can bring each function to full maturity while simultaneously managing risk, allowing them to keep moving forward without getting stuck in a decision-making loop.










5 steps to rolling out a high-value function approach in ServiceNow

Step 01




Identify the organization's high-value functions

Businesses can identify their high-value functions by evaluating risks and their potential impacts on the business. Areas to consider in the identification of high-value functions include:

-  **Financial impacts**
-  **Regulatory impacts**
-  **Product impacts**
-  **Competitor impacts**
-  **Reputational impacts**
-  **Vendor impacts**
-  **Security impacts**
-  **Resiliency impacts**
-  **Staffing impacts**

During this step, organizations consider how large the impact of any given function would be if it were to be compromised. The bigger a function's negative impact is, the higher its value.

 **This can be challenging, but businesses don't have to do it alone. Crowe High Value Function for ServiceNow is a risk management solution that offers standardized criteria assessments to identify high-value functions.**

Step 02



Identify and map the entities that make the function work

Many organizations struggle to identify and map the entities, resources, and assets that work together to enable any given function. This can lead to incomplete asset inventories and uncertainty around what to include in a function set.

That's why it's critical to gain full visibility into each function by performing a cross-departmental analysis to see exactly what makes each function tick. For example, business and IT teams can work together to see where functions overlap across their departments and what roles the teams play in supporting those functions.

Entities to align and map include but are not limited to:



Products



Business processes



Business services



Locations



Vendors



Applications



Servers



Crowe High Value Function provides tailored guides to help organizations document the entity structures and identify dependencies and gaps.

Step 03



Document each function's dependencies and communicate to leadership

All dependencies should be documented in the configuration management database (CMDB) structure so that they can be shared and communicated with leadership, business partners, and operational teams.

Many organizations have part of their business structure outlined but have not documented all of the connections. For example, a company might have a list of business processes and servers identified but be missing all of the locations, applications, or products associated with those systems.

It's important for business leaders and IT leaders to understand the top-down infrastructure supporting their programs and learn how to prioritize key processes and assets.

To map infrastructure for an immature CMDB, they should start by talking to three types of stakeholders:

01 Key process owners

Leaders should diagram the workflow of each process to identify the vendors, locations, and facilities that support the process.

02 Application owners

Leaders should identify the processes, servers, hardware, and any additional applications that support the target application. Vendors, locations, and facilities should also be mapped.

03 Server owners

Leaders should identify the vendors, locations, and facilities that support the server.



Crowe High Value Function offers both automated and manual approaches for documenting dependencies. For mature CMDB data, a company can use Crowe Entity Manager to map each entity and its relationships. For immature or nonexistent CMDBs, a company can load the entity structure through data imports.

Step 04



Use standardized assessments to identify key risks and controls



After identifying the high-value functions and their associated entities, the next step is to identify and align risks and controls associated with each entity.

This lays the foundation for risk and control frameworks. Many organizations will use standardized frameworks such as the [Unified Compliance Framework \(UCF\)](#) to get started. Such existing frameworks easily can be overlaid across functions.

Businesses that don't have an established risk and control framework should ask these key questions before choosing one:

- Do the regulations covered by the content provider align with, and are they filtered down to, the line of business or industry?
- What is the quality of the control statements based on their associated risks and regulations?
- Do the control statements have quality test procedures?
- What is the quality of the risk statements, and do they separate operations and enterprise risk while also highlighting interdependencies?
- Are questions written to align with the risks and controls?



To make it easier to get started, Crowe has created content packs with risk frameworks specifically for Crowe High Value Function.



Step 05



Automate risks and controls

Many organizations stop their programs after identifying key risks and controls, but that's actually one of the least cost-effective points to stop maturing a risk program.

While it's important to have a standardized risk and control framework overlaid across the business and asset inventory, it's also key to take advantage of automation at this stage.

This final step involves evaluating common controls and determining whether the metrics and data that trigger the controls can be automated. ServiceNow makes this easy by allowing businesses to evaluate both internal and external data and write scripts to automate the risk and control testing process.

Here are next steps to take after automating risk and associated control frameworks:

- 01 Continually recalibrate metrics and thresholds related to the risk as additional functions are deployed.**
- 02 Determine which areas can be effectively automated.** Look at each area of automation opportunities: metrics, risk assessment, and control validation processes. Global controls are some of the easiest to automate, and automation methods can be reused as the scope of high-value functions is expanded.
- 03 Start with the most pressing risks, and begin to strategically replicate the automation model to other parts of the program.** Take small steps toward maturity by focusing on getting pieces of the program to a place where risk is managed successfully.
- 04 Check the ServiceNow store for some of the most common integrations, and then use these integrations for quicker automation or results.**



Crowe High Value Function offers a risk and performance monitoring feature to provide an inventory of common key risk indicators and key performance indicators. This allows for full visibility to the status of functions.

Simplify your process and jump-start your risk journey

Maybe you're thinking, "This approach sounds great, but when will I have time to walk my team through these steps?"

 **You don't have to do it alone.**

Crowe High Value Function was designed to work for you and help ease you into risk management. Its strategic top-to-bottom approach guides you in building fully mature risk, security, and IT programs around your most important functions.

In addition, Crowe provides a dedicated team of both technologists and practitioners with deep knowledge of IRM and ServiceNow to help you roll out this innovative risk technology across your organization.





Ready to get started?

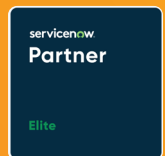
Reach out to our team of Crowe consultants today to learn more about how you can take a high-value function approach to protecting the most important assets of your business.



Jay Reid
Principal, Consulting
jay.reid@crowe.com



Matt Reeves
Managing Director, Consulting
matt.reeves@crowe.com



"Crowe" is the brand name under which the member firms of Crowe Global operate and provide professional services, and those firms together form the Crowe Global network of independent audit, tax, and consulting firms. "Crowe" may be used to refer to individual firms, to several such firms, or to all firms within the Crowe Global network. The Crowe Horwath Global Risk Consulting entities, Crowe Healthcare Risk Consulting LLC, and our affiliate in Grand Cayman are subsidiaries of Crowe LLP. Crowe LLP is an Indiana limited liability partnership and the U.S. member firm of Crowe Global. Services to clients are provided by the individual member firms of Crowe Global, but Crowe Global itself is a Swiss entity that does not provide services to clients. Each member firm is a separate legal entity responsible only for its own acts and omissions and not those of any other Crowe Global network firm or other party. Visit www.crowe.com/disclosure for more information about Crowe LLP, its subsidiaries, and Crowe Global.

The information in this document is not – and is not intended to be – audit, tax, accounting, advisory, risk, performance, consulting, business, financial, investment, legal, or other professional advice. Some firm services may not be available to attest clients. The information is general in nature, based on existing authorities, and is subject to change. The information is not a substitute for professional advice or services, and you should consult a qualified professional adviser before taking any action based on the information. Crowe is not responsible for any loss incurred by any person who relies on the information discussed in this document. © 2023 Crowe LLP.