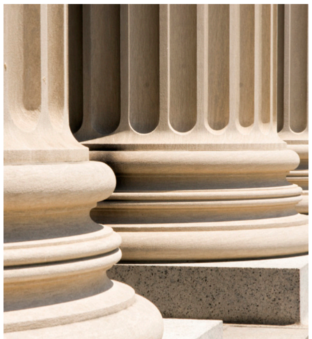
McKinsey&Company

McKinsey Center for Government

Risk-based resource allocation

Focusing regulatory and enforcement efforts where they are needed the most



McKinsey Center for Government

Risk-based resource allocation

Focusing regulatory and enforcement efforts
where they are needed the most

Diana Farrell
Biniam Gebre
Claudia Hudspeth
Andrew Sellgren

February 2013

Contents

Introduction

Many government agencies are responsible for overseeing and monitoring individuals or companies to ensure that they adhere to government rules, regulations, and laws. These agencies have finite resources, so they can't monitor everything all of the time: they have to decide how best to allocate their scarce resources across a broad range of risk exposures. This is called "risk-based resource allocation."

Many different types of government agencies face risk-based resource-allocation decisions. Financial regulators, such as the US Federal Reserve and the Consumer Financial Protection Bureau, oversee thousands of financial institutions to make sure they operate safely, soundly, and fairly. Health and safety regulators, such as the US Federal Aviation Administration, oversee commercial activities to make sure individuals are not exposed to undue risks. And law-enforcement agencies, such as local police departments, monitor wide geographic areas and numerous activities to make sure individuals and companies comply with the law.

While there are significant differences between the missions and operations of these different agencies, they share some common traits: they all seek to protect the public from harm; they all face a virtually unlimited set of potential "targets," or sources of risk; and they all have finite resources with which to monitor and oversee those various targets.

Risk-based resource allocation is more important now than ever, for several reasons. First, as societies have matured, citizens have become ever more insistent on living in safe and predictable conditions. As such, the number of laws and regulations has increased, expanding the scope of necessary enforcement. Second, citizens demand ever more efficiency from government, and so regulatory and enforcement agencies face pressure to fulfill their missions with tighter and tighter budgets.

Examples of government agencies facing risk-based resource-allocation decisions

US Food and Drug Administration: ensuring that drug researchers correctly conduct thousands of clinical trials, affecting hundreds of thousands of subjects

US Department of Housing and Urban Development: ensuring that 5,000 property owners and operators of public and multifamily housing manage housing in a safe and financially responsible manner

US Department of Interior: ensuring that oil and gas producers conduct 2,200 offshore operations in safe and environmentally responsible ways and preventing calamities such as Deepwater Horizon, which cost 11 lives and released 4.9 million barrels of oil

US Internal Revenue Service: organizing 100,000 employees to ensure that 136 million individuals and companies pay the taxes they owe and closing the gap of $385 billion in uncollected taxes each year

US Treasury: ensuring that banks give homeowners appropriate opportunities to modify their mortgages before moving ahead with as many as four million foreclosures each year

The risk-based resource-allocation process

There are four steps in a risk-based resource-allocation process:

1. **Defining the risk:** gaining a deep, clear, and common understanding of the risk exposures the government agency is tasked with addressing

2. **Measuring the exposure:** analyzing data to estimate the risk represented by each individual target

3. **Setting the strategy:** determining how to allocate resources to each individual target, for example, by setting the frequency and depth of inspections

4. **Executing and learning:** conducting risk-management activities, such as inspections, getting feedback on what is working and what is not, and learning from that feedback

As illustrated in Exhibit 1, regulators and enforcement agencies iterate through these steps, refining their approaches over time.

The remainder of this paper illustrates various decisions and good practices in risk-based resource allocation, touching on each of these four areas.

Defining the risk

The risk-based resource-allocation process begins by defining what risks the government agency cares about. This typically flows directly from the mission of the organization, but it is sometimes difficult to enumerate all the varieties of risk, and there is often ambiguity about how to prioritize the risks. One of the best ways to gain clarity and alignment on these topics is through dialogue among the leaders of the government agency.

Keys to success

- **Create a taxonomy of risks.** A taxonomy of risks is a structured list that provides nested levels of detail; see Exhibit 2 for an example. Preparing such a taxonomy helps the government agency to align on a common vocabulary for risks, identify types of risk that might not have occurred before, and prioritize various types of risk.

- **Avoid an undue focus on historical risks.** When an adverse event occurs, it often results in intense scrutiny and

Exhibit 1: Risk-based resource allocation entails four steps

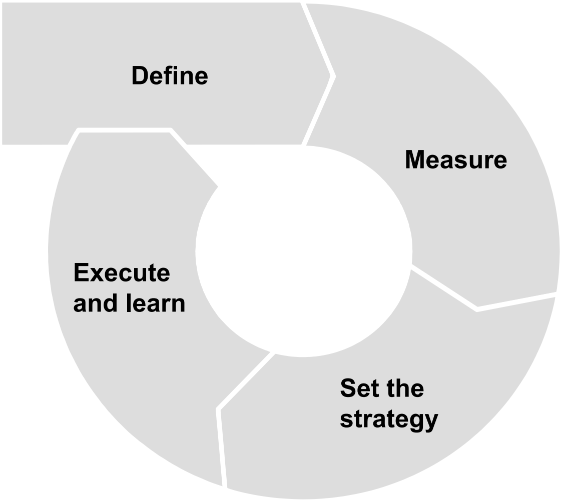
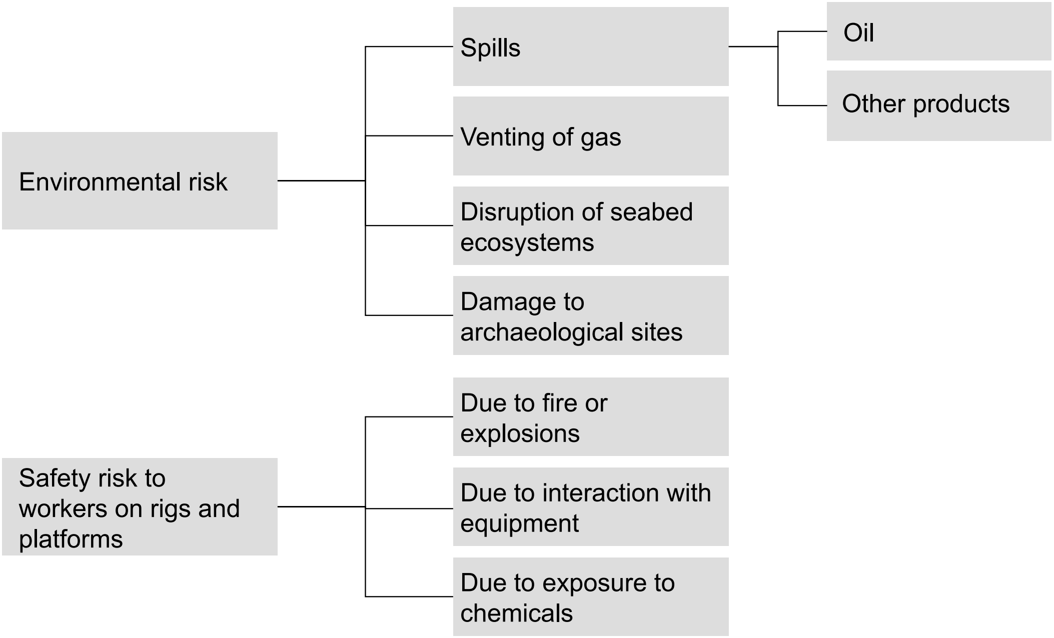


Exhibit 2: A regulator of offshore oil drilling created a taxonomy of risks


Environmental risk
Spills
Oil
Other products
Venting of gas
Disruption of seabed ecosystems
Damage to archaeological sites
Safety risk to workers on rigs and platforms
Due to fire or explosions
Due to interaction with equipment
Due to exposure to chemicals

drives the government agency with oversight over that event to expend significant resources to identify drivers of the event, document deficiencies, and develop processes to prevent the recurrence of similar events. While it is important to prevent adverse events from recurring, it is also important not to lose sight of the fact that future failures are likely to be different. It typically takes a concerted effort by the government agency's leadership to avoid the whole organization focusing on fighting "the last war." After the bombing of the headquarters of the United Nations in Iraq in 2003, UN buildings around the world systematically enhanced security provisions to deter potential car-bomb attacks and mitigate their effects. However, in recent years, attacks on UN offices[1] and residences[2] by suicide bombers and direct assault by armed combatants have outmaneuvered many of the security provisions in place.

- **Formally align on the relative tolerance between false positives and false negatives.** When agencies subject individuals or organizations to additional scrutiny, there are often negative implications for those individuals or organizations. When a safety regulator conducts an inspection of a business enterprise, for example, the inspection often disrupts the operations of the business. The perceived cost of this disruption is higher when the business turns out not to have been doing anything wrong. In this case, targeting the business was a "false positive." On the other hand, the government agency cares deeply about identifying and forestalling all possible adverse

[1] World Food Programme, "Statement on explosion at WFP offices in Islamabad, Pakistan," October 5, 2009.

[2] Allan Woods, "Taliban attacks UN guest house in Kabul," *Toronto Star*, October 28, 2009.

events. Failure to target the business and allowing an adverse event to occur is a “false negative” result, which can lead to loss of life or other calamities. It is imperative to forge clarity among the government agency’s leadership about how much the agency can tolerate both false negatives and false positives so that the resource-allocation approach can balance the risks appropriately.

Measuring the exposure

Estimating the level of risk posed by specific targets is a critical input for prioritizing the deployment of constrained resources. The first step in measuring the risk is to identify an expansive set of possible drivers of risk. For example, a bank regulator might determine that a bank is more likely to fail if it holds too great a concentration of assets in any one industry. In our experience, one of the best ways to generate an expansive set of possible drivers is to convene a workshop with subject-matter experts who have built up intuition about the drivers of risk through years of experience.

The second step in measuring the risk is to get historical data on those drivers and to understand what risks were in fact realized. The bank regulator, for instance, would get historical data for all banks over many years, looking at the assets they held and determining why each bank failed.

The third step is to conduct statistical analysis to determine which of the possible drivers actually predict adverse events, and thereby to determine the sensitivity of risk to those drivers. The output of this analysis, then, generally is a kind of scorecard that lists 5 to 15 drivers of risk, with weights or a formula for combining the various drivers into an overall risk score.

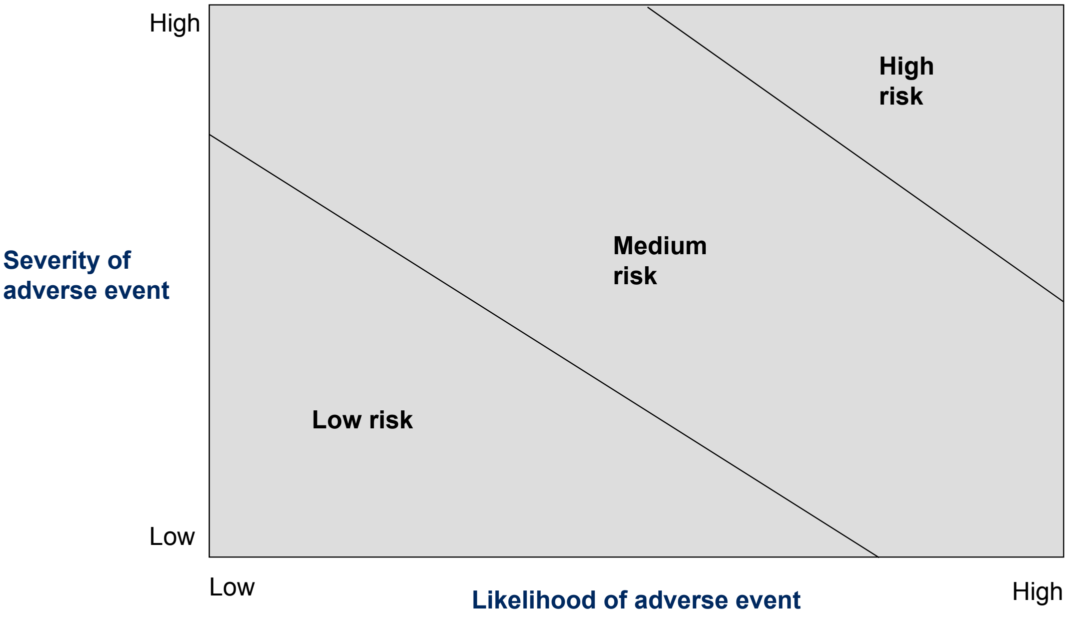
Sometimes it’s not possible to get historical data on drivers and outcomes, and so statistical analysis is not possible. In these cases, one typically convenes a group of experts in the risks involved to formalize their intuitive judgment, based on years of experience, about which risks matter and how to weight them.

Keys to success

- **Measure both the likelihood and severity of adverse events.** If an adverse event is very likely but the damage would be minimal, then the event is not a major concern. Similarly, an event that would cause serious calamity doesn’t warrant a lot of attention if it’s logically not possible for it to occur. In our experience, it is good practice to calculate and manage according to the “expected loss” from an adverse event, which is defined as the product of likelihood and severity (Exhibit 3). Notably, the severity of an adverse event is often proportional to the size of an organization or operation. For a food-safety regulator, for instance, the risk of a given food or beverage product is usually proportional to the number of people who consume it.

- **Work backward from as many adverse events as you can.** Past failures are often a rich source of ideas about how adverse events can happen. This is particularly true in situations in which there are many smaller adverse events that happen frequently, rather than a few larger adverse events that happen rarely. In the health care arena, for example, the Department of Veterans Affairs National Center for Patient Safety develops tools for conducting root-cause-analysis investigations for all patient-safety issues, including medication errors, patient mistriage, and other adverse

Exhibit 3: Expected loss is the product of likelihood and severity of an event.



outcomes.[3] Multidisciplinary root-cause-analysis teams investigate both actual adverse events and situations in which a process error occurred, even if there wasn't a negative outcome for the patient.

- **Learn from adverse events that happened but that were not detected.** Bank failures and terrorist attacks are adverse events that will be detected almost all of the time, but many adverse events go undetected. For instance, many people cheat on their taxes without getting caught. Exploring drivers of only the detected adverse events would incorrectly focus attention on a subset of the true risks. A powerful way to overcome this challenge is to create a sample of targets, scrutinize each sample target extremely rigorously, and then use this sample to identify the risk drivers. Suppose a tax authority's normal processes detect errors in 2 percent of tax returns, for example. The other 98 percent of returns might also contain errors. The tax authority might do an extraordinarily detailed audit of 1,000 cases as a one-time exercise and find 30 returns with errors. The normal processes would have identified 20 of those errors, but the deeper audit found 10 additional errors. The tax authority would then use the 30 returns to identify the drivers of risk.

- **Take care to identify the drivers of risks that have not yet happened.** A data-driven approach is inherently backward looking and is not able to predict events that have never occurred. For example, before September 11, 2001, the world had never experienced hijackers using planes to destroy buildings, and so statistical analysis of the risks posed by people who bought one-way

[3] J. Bagian et al., "The Veterans Affairs root cause analysis system in action," *Joint Commission Journal on Quality and Patient Safety*, 2002, Volume 28, Number 10, pp. 531–45.

plane tickets would not have identified that risk. In such situations, it is imperative to augment data-driven approaches with creative judgment about risks that have never happened. This can be done effectively by convening workshops with seasoned experts and by using various brainstorming approaches, such as issue trees, and calibration approaches, such as the Delphi method.

- **Try to counteract cognitive biases.** Research into human psychology and behavioral economics has shown that humans have biases that lead them to underestimate particular types of risk. These biases include the following:

  — **Hindsight bias.** People assign probabilities that are too high to events that have occurred before and too low to events that have never occurred.

  — **Optimism bias.** People tend to underestimate the probabilities of bad events befalling them, thinking that such bad events are more likely to happen to other people.[4]

  — **The availability heuristic.** People tend to underestimate the prevalence of things that are no longer visible today, such as an oil spill that has been cleaned up, and so they tend to underestimate the likelihood of adverse events that don't leave visible scars in the long term.

  — **The representativeness heuristic.** People tend to think about the typical or average outcome more than unusual outcomes or outliers, and so they typically underestimate risks of unusual or extreme events.

  — **The illusion of control.** People tend to overestimate their ability to control events and thus underestimate the likelihood of negative events over which they have some control.

  Several practices help to counteract these biases:

  — educating those who are conducting risk assessments to make them aware of these biases

  — having more people involved in risk assessment to create an environment in which individuals will challenge one another's biases

  — infusing risk assessments with as much objective data as possible, in order to make biases more transparent

- **Get data and input from a wide variety of sources.** Regulators and enforcement agencies operate in a world of imperfect information: they can't watch every target all of the time. As such, it is imperative for these agencies to take advantage of freely available information, implement processes to gather useful information quickly and easily, and organize themselves internally to

[4] See N. D. Weinstein, "Unrealistic optimism about susceptibility to health problems: Conclusions from a community-wide sample," *Journal of Behavioral Medicine*, 1987, Volume 10, Number 5, pp. 481–500. The study showed that the perceived ratio of below-average to above-average risk was 9:1 for asthma, 8:1 for drug addiction, and 7:1 for food poisoning, for example. See also H. Pentecost, P. Price, and R. Voth, "Perceived event frequency and the optimistic bias: Evidence for a two-process model of personal risk judgments," *Journal of Experimental Social Psychology*, 2002, Volume 38, Issue 3, pp. 242–52.

ensure that information flows seamlessly within the agency to those who would use it to make resource-allocation decisions.

For example, in the case of the Ponzi scheme propagated by the Bernard L. Madoff Investment Fund, the US Securities and Exchange Commission (SEC) received six complaints from a variety of sources between June 1992 and December 2008 on the viability of the fund's returns and operations. Furthermore, two articles published in 2001 raised flags regarding "Madoff's unusually consistent returns."[5] Based on the series of complaints received, the SEC launched several investigations into Madoff's fund, the first of which was in 1992—but the SEC investigative teams relied largely on information from Madoff himself rather than collating third-party evidence that would have exposed the fraudulent activities.[6] As a result, the scheme was left to operate for more than 16 years, until it collapsed in 2008, resulting in cash losses in excess of $70 billion.[7]

Setting the strategy

Once the risks have been defined and measured, the government agency needs to decide on an optimal strategy to deal with those risks.

Before any adverse event happens, the government agency should have a strategy to mitigate the risks by decreasing both the likelihood and severity of an adverse event. One of the primary ways to decrease the likelihood of an adverse event is to implement controls that discourage dangerous behaviors. For instance, an agency responsible for airline safety might put bomb-detection equipment in airports, or a bank regulator might require each bank to document any large cash deposits to prevent money laundering.

Decreasing the severity of future adverse events is also important. For example, after the 1971 San Fernando Valley earthquake, which claimed 58 lives and caused widespread damage, the state of California made changes to its building codes, requiring retrofits of unreinforced-masonry buildings with the greatest risk of collapse.[8] These efforts paid off in the 1994 Northridge quake, when there were no fatalities among the 200,000 people who lived in the 1,300 buildings that had been retrofitted.[9]

Often, it is not immediately obvious that an adverse event has occurred. In these cases, the government agency should develop a strategy that consciously sets out to detect such events. The first reported "drug mule," for instance, was discovered in 1973 by doctors in Toronto, Canada, who admitted a patient with a bowel obstruction 13 days after he had swallowed a hashish-filled condom. Prior to that, border officials worldwide were not aware of the method of "body packing" as a means of transporting illicit drugs. Since then, internal concealment has become a major strategy to move

[5] D. Kotz, Investigation of *Failure of the SEC to Uncover Bernard Madoff's Ponzi Scheme*, SEC Office of Inspector General Report of Investigation, case number OIG-509, 2009.

[6] Ibid.

[7] Securities Investor Protection Corporation v. Bernard L. Madoff Investment Securities LLC, number 08-01789 (BRL), US Bankruptcy Court Southern District of New York, 2010.

[8] Tony Knight, "'71 quake's lasting impact: Sylmar temblor forever changed scientific perceptions, public's attitudes," *Los Angeles Daily News*, February 9, 1996.

[9] Ibid.

high-value drugs, such as cocaine and heroin,[10] and border officials have responded by putting new detection methods in place.

Once the government agency identifies violations, it needs to decide what to do with the responsible party, which can be anything from providing helpful education to imposing stiff penalties. Of course, how the agency handles identified violations has important implications for the likelihood of future violations.

Keys to success

- **Implement thoughtful controls.** In principle, the best-designed controls are capable of preventing every future violation, and so they are often quite efficient. For example, one of the most efficient and effective controls was imposed by the US Internal Revenue Service (IRS). Individual US taxpayers had long benefited from tax deductions for each dependent under their care. The IRS suspected that many taxpayers were claiming too many dependents; starting with the 1987 tax year, the IRS required each taxpayer to provide the IRS with the tax identification number (TIN) of each dependent for whom that taxpayer claimed a deduction. This program was known colloquially as "TINs for tots."[11] By requiring TINs, the IRS was able to verify that all the claimed dependents actually existed and were claimed on no more than one tax return. In the first year of this control being in place, the number of claimed dependents in the United States fell by seven million children, even before the IRS verified the dependent data.[12] Collecting this extra information cost tax filers and the IRS almost nothing, yet it was extremely effective at bolstering compliance.

- **When adverse events are difficult to forestall, focus on mitigating the damage.** Regulators and enforcement agencies often face "asymmetric" risks, where adverse events are more likely to occur wherever the government agency is not focusing. Criminals tend to rob the least-protected target, for instance. While vigilant detection efforts are essential in such cases, it is often more cost-effective to focus on mitigating the damage from an adverse event. For example, the US Department of Homeland Security has worked with the University of Southern Mississippi to create a model for an evacuation simulation for the security management of university sports venues, leading to recommendations regarding emergency-response capabilities and contingency planning to ensure business continuity in the event of a major incident.[13]

- **Allocate detection efforts based on risk.** When allocating resources to ensure that controls are in place and to detect actual violations, agencies should focus their resources wherever the risks are the greatest. This might seem like an obvious point, but it is a powerful driver of efficiency

[10] According to one article, "Every year, roughly three thousand people are arrested while working as 'mules' smuggling drugs through the ports of entry along the US-Mexico border in California, Arizona, New Mexico, and Texas. For every mule caught, many more get through." See D. Bjerk and C. Mason, "The market for mules: Risk and compensation of cross-border drug couriers," Social Science Research Network, 1881212, July 7, 2011.

[11] N. Dunnan, "Beware the ides of April: Changes in effect for the new tax season," *ABA Journal*, 1992, Volume 78, Issue 3, p. 77.

[12] J. Szilagyi, "Where some of those dependents went," *Internal Revenue Service 1990 Research Conference Report: How Do We Affect Taxpayer Behavior*, March 1991, pp. 162–3.

[13] South East Region Research Initiative, "Program review, March 25–26, 2009."

and effectiveness, and most government agencies only loosely focus their efforts in this way. Exhibit 4 shows an example of a government agency that has room to improve its risk-based resource allocation.

- **When potential violators are sophisticated, focus more deeply on fewer targets.** The returns to investigative effort on any given case generally follow an “S-shaped” curve: there are low returns to investigative resources at first, because the government agency doesn’t understand the case well enough to identify bad behavior. Then there is a “sweet spot,” the steepest part of the curve, where the agency understands the case and quickly identifies bad behavior. Then there are once again low returns to additional resources, because the agency has already identified most of the bad behavior (Exhibit 5). For sophisticated targets that expend significant resources to avoid detection, this curve tends to be lower and to the right. The optimal amount of resources to expend on each case depends on the shape and location of the curve. For unsophisticated targets, the agency should spend fewer resources on each case and scrutinize many cases; for sophisticated targets, conversely, the agency should invest more resources and consider fewer cases.

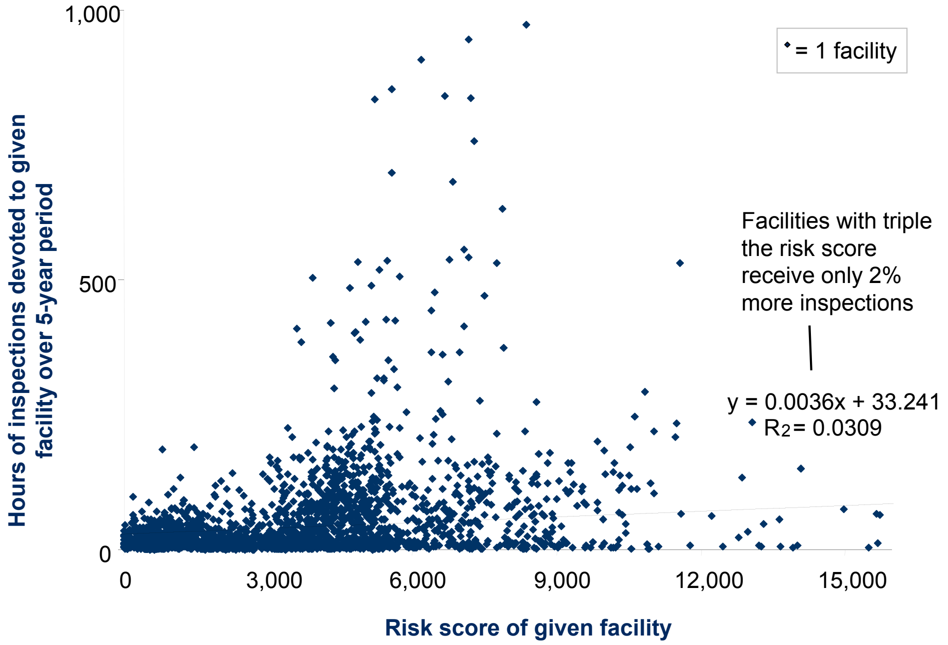
- **When potential violators could remediate violations quickly, use random inspections.** Here, government agencies have to strike a balance between efficiency and effectiveness. It is almost always more efficient for inspection efforts to be planned well in advance, so that the inspected party can have the requisite information ready and have cleared time to interact with the agency. On the other hand, if a violator knows that an inspector is coming, that violator will make every effort to conceal or remediate bad behavior, making the inspection less effective. Generally, when it is difficult to conceal or remediate bad behavior, the agency should favor the efficiency of planned inspections. For example, for individuals who are seeking a commercial driver’s license, the US Federal Motor Carrier Safety Administration conducts random and surprise testing for the use of drugs and alcohol.[14] As a counterexample, building inspectors tasked with ensuring safe construction standards can use scheduled inspections, since things like the spacing of wall studs will be apparent to the inspector, and there’s nothing the builder can do hide noncompliance.

- **Inspect both broadly and deeply.** The government agency should measure a given set of variables consistently over time to get a holistic picture of activities and to enable it to draw inferences about how behavior may be changing. The agency should then augment this common set of measures with periodic deeper investigations into particular topics to identify any abnormalities or violations that might be obscured at the aggregate level. For example, financial regulators in the United States consistently review the capital levels of banks to identify worrying trends, but those regulators also conduct deeper periodic “horizontal reviews” on specific topics, such as subprime lending.

- **Educate violators who have good intentions.** When it is reasonable to judge that violations were unintentional, there is an opportunity for the government agency to improve compliance through education, by making instructions clearer or by notifying the parties of their noncompliant behavior. Dynamic-speed-display signs, for instance, display the speed of an approaching vehicle and sometimes a message for the driver, such as “slow down.” These displays have been

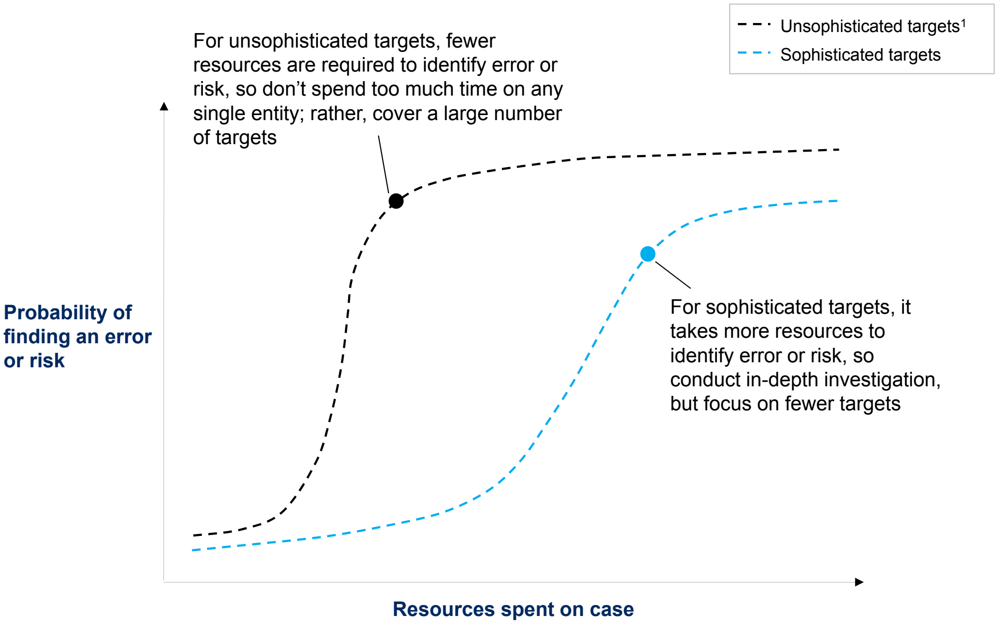
[14] US Department of Transportation, Federal Motor Carrier Safety Administration, “Controlled substances and alcohol use and testing,” *US Federal Register*, August 17, 2001.

Exhibit 4: Focus resources on the largest risks



Source: Regulator data; McKinsey analysis

Exhibit 5: For sophisticated targets, conduct deeper inspections



[1] Unsophisticated targets do not actively avoid detection, do not modify their behavior in response to detection efforts, and spend less avoiding detection than the government spends detecting the targets.

shown to reduce average speed by 1.1 to 5.7 miles per hour[15] and to reduce the number of drivers exceeding the speed limit by as much as 38 percent.[16]

- **Punish violators who have bad intentions.** When violations are intentional, the government needs to change the incentives of the violating parties to make it rational for them to comply. Often, the most efficient way for the government to do this is to pursue select high-profile cases and publicize those efforts. On October 12, 2006, for example, actor Wesley Snipes was charged with conspiring to defraud the United States by making false and fraudulent claims for payment against the United States and by failing to file federal income-tax returns from 1999 to 2004.[17] The IRS publicly highlighted the Snipes case as one of the success stories of the new Tax Defier Initiative of 2008.[18]

Executing the risk-management plan

Most agencies operate in a complex and dynamic environment, where there are unlimited opportunities to improve and the risks change over time. As such, agencies should design operating models that foster communication and learning.

Keys to success

- **Establish feedback processes.** As discussed earlier, risk measurement involves aggregating and analyzing data from disparate sources, with complex interactions, in environments that change over time. Accordingly, the government agency should constantly foster feedback on its measurement and detection of risk. For example, it's often the case that data-driven risk assessment is conducted at the agency's headquarters, while field personnel interact directly with the risks themselves. In such instances, it is extremely helpful to establish regular dialogue between the field and headquarters personnel, so field personnel can inform risk analysts about what is and isn't being picked up in centrally provided risk assessments. At the same time, the risk analysts can inform field personnel of emerging trends and patterns in data across the government agency.

- **Build a culture that delivers continuous improvement.** No government agency has created a perfect system to allocate resources in our uncertain and ever-changing world. As such, agencies should strive to create a culture of continuous improvement, focusing on each of the four steps in risk-based resource allocation: defining the risk, measuring the risk, setting the strategy to manage the risk, and executing that strategy.

[15] City of Bellevue, Washington, Transportation Department, *Stationary Radar Sign Program Report*, 2005.

[16] S. Stern et al., "Evaluation of the dialog display, Berlin studies," *Zeitschrift für Verkehrssicherheit*, 2010, Volume 56, pp. 115–22.

[17] Tony Norman, "Dear Wesley Snipes: Next time, try Wall Street," *The Pittsburgh Post-Gazette*, December 3, 2010.

[18] US Department of Justice, "Wesley Snipes among government's biggest tax cheats of 2008," April 14, 2009.

Conclusion

Government is increasingly called on to protect the public from harm and to shield society and the economy from volatility, but to do so as efficiently as possible. Adopting good practices in risk-based resource allocation is a powerful way for regulators and enforcement agencies to meet their missions efficiently and effectively.

Diana Farrell is a director in McKinsey's Washington, DC, office, where **Biniam Gebre** is a principal, **Claudia Hudspeth** is a consultant, and **Andrew Sellgren** is a principal.

Contact for distribution: Francine Martin
Phone: +1 (514) 939-6940
E-mail: francine_martin@mckinsey.com

McKinsey Center for Government
February 2013
Layout by New Media Australia

www.mckinsey.com/mcg