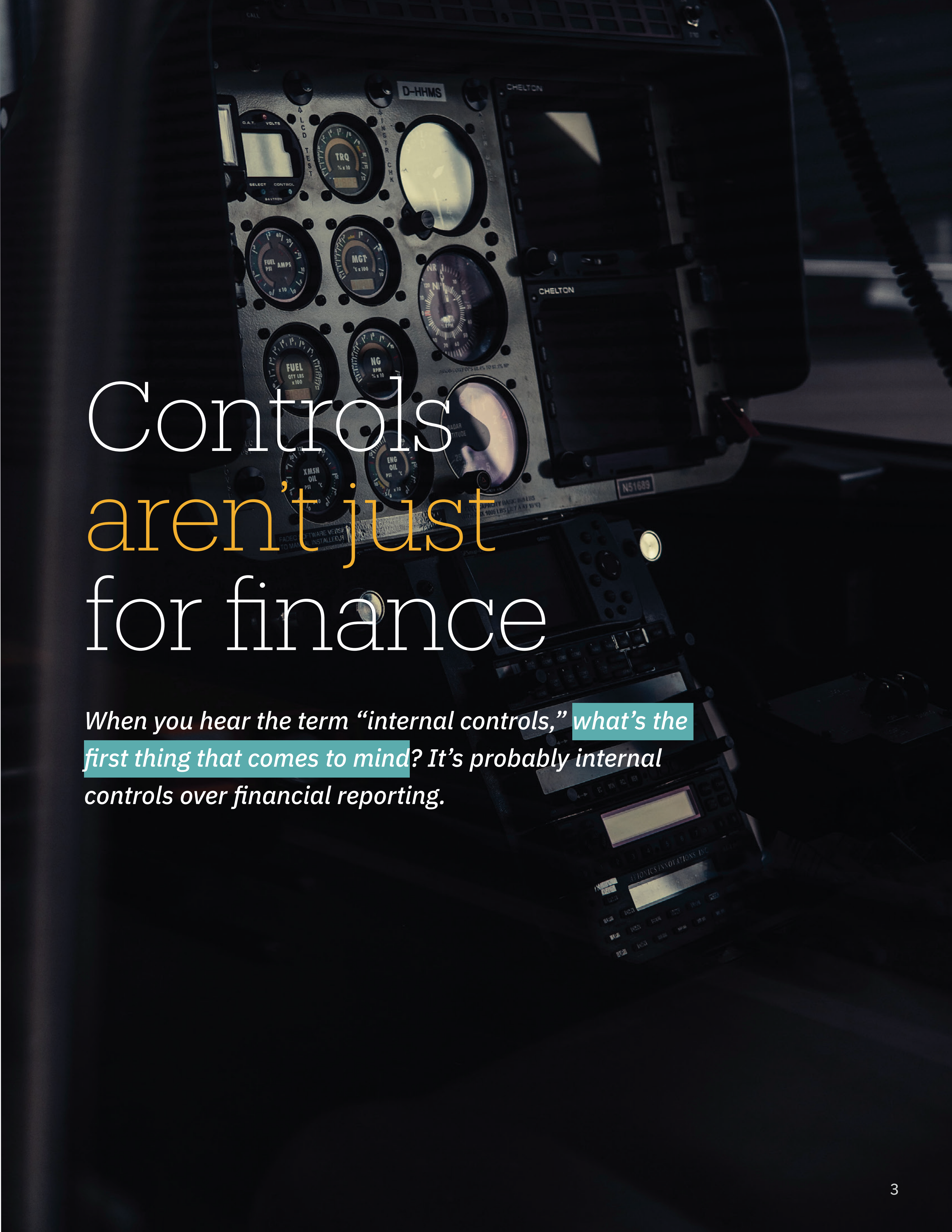
Galvanize

Reaching internal controls utopia

Expanding internal controls to drive a more successful organization

Table of contents



Controls aren’t just for finance

When you hear the term “internal controls,” what’s the first thing that comes to mind? It’s probably internal controls over financial reporting.

In fact, if you search for the definition of internal controls, you'll mostly see something like:

> Internal controls are the mechanisms, rules, and procedures implemented by a company to ensure the integrity of financial and accounting information, promote accountability, and prevent fraud.[1]

This and similar definitions lead people to assume that internal control is only the domain of finance and audit—and other business areas aren't involved in it. But, when you think about it, finance and accounting are a window into the workings of the entire organization, and internal audit (which provides assurance over finance) is mainly concerned with how the entire organization is managed.

So that said, every single department and employee must embed and use internal controls to protect assets and intellectual property, reduce duplication of work, and report efficiently—things that are definitely not restricted to the finance and audit departments. Actually, the industry recognized COSO Framework[2] provides comprehensive guidance for organizations to use in developing an internal control system for non-financial reporting. This guidance also helps improve existing operational controls.

And, thinking quickly about your own organization, you could probably identify many controls outside of finance. In fact, your organization couldn't really operate without them. For example, it's hard to recruit new employees without first adhering to hiring guidelines, or to sell a product without contract processes firmly in place. But in many organizations, these controls are often lacking because of poor design, implementation, or maintenance.

If that's the case, why not strategize and implement internal controls across the organization to work in harmony? After all, they help an organization run efficiently and effectively. What are the barriers? And what are the steps to implementing a sound, effective system? To find the answers, we looked at multiple best practices, standards, and frameworks (particularly COSO), and examined our own experience working with clients from around the world.

> ***Internal control is more than simply ticking boxes. It's about doing what's right for the organization so it can meet its business objectives. This means internal controls need to be baked into the core of every employee's job.***

[1] **Investopedia,** *2019, Internal controls*

[2] **PwC,** *2016, COSO for non-financial reporting: More transparency, more trust*

The emerging "change risk" challenge

Change is the greatest challenge to effective internal controls.

New tech and innovative ideas have disrupted business models and there's no sign of this slowing down. Organizations need to keep up and respond quickly to adapt to these new environments. But this increases risk. From the internet of things (IoT) to machine learning, artificial intelligence, and robotic process automation, emerging technologies introduce constantly evolving and growing challenges.

We're increasingly more connected to the external world, and as a result, more exposed to infiltration and manipulation threats, whether intentional or not.

At the same time, insider threats—both unintentional and deliberate—have increased, fuelled by the constant pressure to cut costs, improve profits, and do more with fewer resources.

New dangers like cyber risk and climate risk are keeping top management awake at night. In many organizations, these risks have now secured a place on the board's agenda. With the risk landscape changing all the time, we'd even go so far as taking all of these risks and chucking them into a "change risk" bucket.

Controls create more productive organizations

Controls are so much more than just mechanisms to protect against threats.

They actually help organizations run better. Yet many organizations get lost in designing controls that focus on prevention within a specific role or department, rather than on promoting organization-wide efficiencies and performance like these:

- Mandatory training for new employees to learn standard operating procedures (HR).
- Bi-annual townhalls to share organizational objectives and plans with the entire workforce (operations).
- A clearly defined approval process for any public-facing brand messaging (marketing).
- Bi-annual mandatory employee security training (IT security).

No matter which department or team implements them, at their core internal controls:

- Manage risks and mitigate threats
- Steer organizational activity toward objectives
- Create trust and confidence
- Help to comply with laws and regulations.

BUT SOMETIMES CONTROLS FAIL

Controls often fail as a result of three main factors: people, process, or technology. And any control can easily sink if it's not well designed or implemented; or enforced, monitored, tested, and regularly updated.

If you don't test, service, and repair/replace your car's brakes periodically, your crash risk increases. This is similar for internal controls—if you don't regularly test them to make sure they're relevant, reliable, and working, the chances of failure grow.

MATERIAL WEAKNESSES LEAD TO CONTROL FAILURES

A material weakness occurs when one or more of a company's internal controls is ineffective. But why is this a big deal? Well, if a material weakness goes undetected or isn't resolved, a material misstatement could happen in an organization's financial statements. This can then have the snowball effect of impacting an organization's valuation or financial performance.

In October 2018, Costco Wholesale reported a material weakness in its IT general controls. In a statement released by the company, it revealed that unauthorized people may have gained access to the company's financial reporting systems. Costco reported that although they took immediate action to rectify the material weakness, remediation would continue throughout 2019.

So, what impact did this have? Immediately following the announcement, Costco's stock price fell by 4%.

EXAMPLES OF CONTROL FAILURES

Employees—those who are dishonest or just trying to get their jobs done—can circumvent even well-designed controls, so it's important to review the actual functioning of the controls from time to time.

Moody's[3]

In August 2018, Moody's agreed to pay $16.25 million to settle charges of internal controls failures involving models it used to rate US residential mortgage-backed securities (RMBS).

According to the SEC's order, Moody's failed to establish and document an effective internal control structure for models they had outsourced and used in rating RMBS from 2010–13. They also failed to maintain and enforce existing internal controls that should have been applied to the models. Ultimately, Moody's corrected more than 650 RMBS ratings with a notional value exceeding $49 billion, due in part to errors in the models. They now retain an independent consultant to assess and improve internal controls.

Citigroup[4]

The SEC charged Citigroup $4.75 million for deficient internal controls at subsidiary Grupo Financiero Banamex, S.A. de C.V. (Banamex). Banamex loaned $3.3 billion to Oceanografia, S.A. (OSA). The funds were advanced to OSA based on invoices and work estimates for services it provided to oil company Petroleos Mexicanos (Pemex) between 2008 and 2014.

However, some of the factored documents that Banamex received from OSA, amounting to about $400 million, were fraudulent and included forged signatures. Banamex lacked the controls necessary to test the authenticity of the factored documents prior to advancing OSA the funds.

The bank agreed to pay a $4.75 million penalty to settle the SEC's charges. It did so without admitting or denying the SEC's findings and agreed to cease and desist from future violations.

[3] **Internal Audit 360,** *2018, Moody's to pay $16 million for internal control failures*

[4] **CFO,** *2018, SEC charges Citigroup for internal controls failure*

Creating a sound internal control system

To avoid headline-grabbing control failures, here are four steps to follow when creating your internal control system.

01

Assess where you are (plan)

Use the COSO Internal Control cube[5] and the maturity model (see Figure 1) to understand and define the current state of internal control. Look at how your company is achieving its objectives with operations, reporting, and compliance. Assessments should include the state of the control environment, corporate culture around risk and controls (tone at the top), risk management and control activities, and monitoring activities. The findings will help you define the maturity level for your company.

02

Make sure you have the right stuff & get started (resource & implement)

At this stage, it's critical to make sure you have enough resources to develop and implement the plan. Do you have the budget? The people? The time? The technology? Identifying and securing these resources can be a lot of work.

03

Agree on where you want to go (communicate & align)

Decide where you want to be using the maturity model as your guide (informal/ad hoc, standard, managed and monitored, optimized). This decision should be made by top management and preferably in consultation with the auditors. The auditors always report on the state of internal control, so they're a great resource and guide to start creating an action plan.

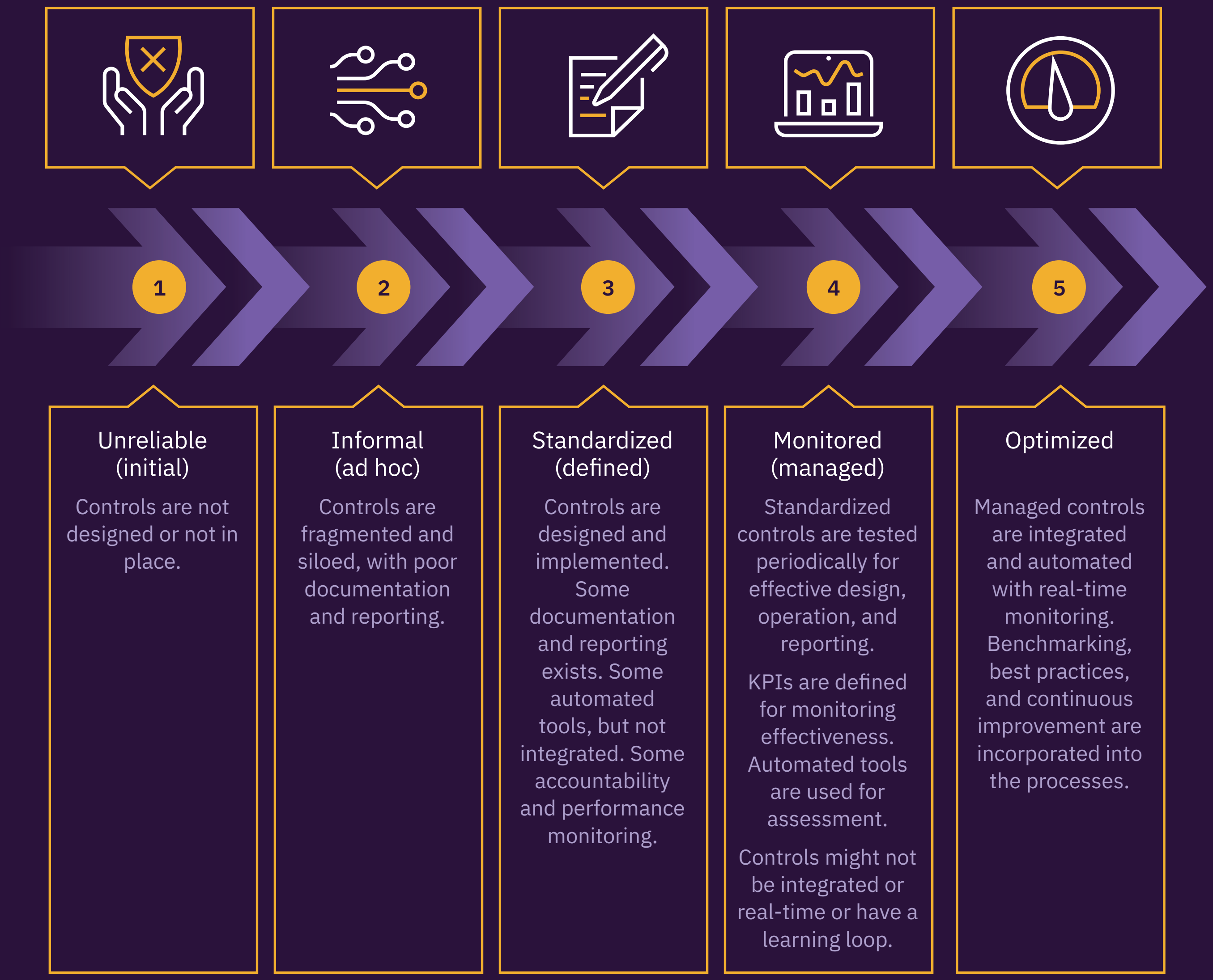
04

Roll out & refine your plan (review & test)

Depending on how involved your plan is, the rollout can take months or even years. Reviewing and testing must be done on an ongoing basis—this is not a "set-it-and-forget-it" kind of program.

[5] **COSO Internal Control —Integrated Framework Principles,** *https://www.coso.org/Documents/COSO-ICIF-11x17-Cube-Graphic.pdf*

FIGURE 1: INTERNAL CONTROLS MATURITY MODEL



Unreliable (initial)

Controls are not designed or not in place.

Informal (ad hoc)

Controls are fragmented and siloed, with poor documentation and reporting.

Standardized (defined)

Controls are designed and implemented. Some documentation and reporting exists. Some automated tools, but not integrated. Some accountability and performance monitoring.

Monitored (managed)

Standardized controls are tested periodically for effective design, operation, and reporting.

KPIs are defined for monitoring effectiveness. Automated tools are used for assessment.

Controls might not be integrated or real-time or have a learning loop.

Optimized

Managed controls are integrated and automated with real-time monitoring. Benchmarking, best practices, and continuous improvement are incorporated into the processes.

Reaching a state of internal controls utopia—where the entire organization works together in harmony—can be fraught with challenges ... like getting full buy-in from senior management, availability of timely resources and technology, obtaining the required data, working with different teams or people, and of course, change management.

You need to face these challenges head-on and that happens through mindful and inclusive planning, implementation, review, and testing.

How risk drives control design

Controls aren't cheap and they require people, processes, and technology resources.

To make sure your plan is laser focused, do a risk assessment—using a combination of qualitative and quantitative methodologies—to prioritize and implement controls that mitigate the most critical risks first. This would be taking a risk-based approach, similar to how auditors address their work.

It makes sense, because if there was no risk, there'd be no need for controls. Risk and controls are tightly coupled, so this means good risk assessment is crucial for implementing a solid controls system.

01

Prioritize & score your risks by likelihood, impact, & affect

Classify and categorize your assets according to their criticality. According to Risk in Focus 2019,[6] some of the top risks (likely to occur with a major impact on business assets) include:

TOP RISKS	IMPACTS FROM THESE RISKS	BUSINESS ASSETS AFFECTED
Cybersecurity	Data breaches	Compromised R&D/confidential info
Data security and protection	Customer dissatisfaction	Loss of revenue
HR and people risk	Operational failure due to lack of resources	Loss of people and intellectual property
Regulatory change	Increased workload, slowing of other work	Dilution of workforce
Innovation	New machinery or facilities required	Outdated or old machinery or facilities
Culture	Inability to hire	Loss of employees
Outsourcing and third parties	Hacking	IT hardware and networks
Supply chains	Breach of child labor or unsafe materials laws	Loss of revenue
Environment/climate change	Flooding, acts of God, fire	Buildings, contents, data, and records

(To learn more about risk assessments, we suggest reviewing COSO's Enterprise Risk Management – Integrated Framework and adapting it to your specific needs.)

[6] **Chartered Institute of Internal Auditors,** *2019, Risk in focus 2019*

02

Classify & categorize controls into preventive, detective, or reactive

In terms of operational effectiveness, one is the highest control category and seven is the lowest. The higher the category, the quicker the control neutralizes the threat and reduces the impact.

CATEGORY	ABILITY TO DETECT THE EVENT & TAKE RECOVERY ACTION	TYPE
1	Prevents the event or detects it as it happens and prevents further impact.	Preventive
2	Detects the event and reacts fast enough to fix it well within the time window.	Detective
3	Detects the event and reacts fast enough to fix it just within the time window.	Detective
4	Detects the event but can't react fast enough to fix it within the time window.	Detective
5	Fails to detect the event but has a partially deployed recovery plan.	Reactive
6	Fails to detect the event but does have a recovery plan that can be deployed.	Reactive
7	Fails to detect the event and doesn't have a recovery plan.	Reactive

Looking at this chart, you might think that using a preventive control all the time would be ideal. You'd be wrong.

03

Factor in cost

It's all about the cost effectiveness of controls. If the cost of using a preventive control (the highest category of control) is less than the cost to fix the issue (and any possible impact penalties for all the events that control is designed for), then use it. The costs of using a preventive control include the expense to buy/develop, install, configure, commission, operate, and maintain it, as well as the costs to train people and audit its use. A similar cost analysis would be needed when considering detective and reactive controls, after which the decision to deploy the control is then taken.

04

Get rid of redundant controls

Redundant controls are costly, time-consuming, and result in duplicate work. So it's best to identify, avoid, or eliminate controls for those individual risks or events that are universally addressed by some other control. Or controls that don't actually address any specific risk or event. If a control is truly redundant, its removal should lead to improvements in cost effectiveness.

05

Focus on segregation of duties

Fraud regularly happens when too much authority is given to one employee, so it's essential that duties and tasks are performed by different people. One employee shouldn't have the authority to create a new vendor, as well as the ability to enter a transaction to pay that vendor. With the authority to perform both tasks, they could create and pay a fake vendor.

In manual systems you'd require people to review one another's work. In an automated system, where duties are separated and assigned by role, employees can only perform the task(s) defined in their assigned roles, reducing the need for manual oversight.

06

Automate all the things

Using risk management software is the best way to automate your internal controls. It helps prioritize risks based on severity and likelihood, which means controls are also prioritized. It gathers your risks and controls together in one library, removing duplicated data and effort.

Automated preventive controls include:

- Forced scheduled passwords updates.
- Regular security policy review and attestation.
- Assigning authorization amounts and preventing users from entering amounts that exceed those.

Examples of automated detective controls:

- Use intrusion detection or anti-virus software to find exceptional activity and create automatic reports. (These can double as corrective controls when they kill or quarantine the intruder or virus.)
- Use an automated audit system to scan data for deviations against policies and regulations, and highlight them in a report or a dashboard. For example, the audit solution could be set up to scan your ERP data to highlight entries made outside office hours. The system takes action automatically when a risk event occurs. An alert email or SMS could be sent automatically for action or those entries could even be quarantined or deleted.

07

Set up self-policing procedures

Audit is a useful mechanism for evaluating the effectiveness of internal controls, but self-policing procedures—especially when automated—go a long way in helping to create and maintain an effective internal control system. Self-policing procedures quickly detect control failures, allowing other controls (reactive controls) to take over.

Let’s say you have a preventive control that limits the amounts you’re authorized to enter in the financial system. But something strange happens, and you can now enter an unauthorized amount. The reactive control would fire an email to your manager informing them of the entry so they could follow up immediately. In addition, all entries above a certain amount would need their authorization before being paid or posted in the books.

If a control is not protected by a self-policing procedure, a control failure may go undetected and become a big problem. Note that self-policing and fail-safe properties are requirements of the higher-order categories of control systems (refer to the control category table in step 2).

When selecting an internal control, you should document it for how and why that particular control was chosen. ISACA has produced an internal control selection worksheet[7] that can be used for this.

[7] **ISACA,** *2016, Internal and mitigating control selection worksheet*

Plan to fail

Even mature organizations experience control failures. (It happens, don't take it personally.)

This is why you'll want to have a contingency plan. Something that will allow you to act quickly and minimize any damage.

What would the impact penalty be if the unthinkable was to happen? Having answered that, the next question is, is that an acceptable risk? If not, then you need a contingency/business continuity plan.

Let's imagine your IT team has just completed an audit. The IT audit reports that the IT team only reviews privileged access (PA) once a year. This raises a red flag, so you start doing some digging and find several people who have access to sensitive customer information. Information they shouldn't be allowed to (and don't need to) access.

The control to review PA once a year was implemented a few years ago, when the organization was smaller and didn't need to comply with as many regulations. In this sense, the control failed because it wasn't regularly reviewed. It also wasn't tested to make sure it was still relevant as the organization grew and changed.

The control is broken, so now what? What are your next steps? This is where you'd turn to your prepared (and tested) contingency plan.

> "If you fail to plan, you are planning to fail."
>
> » ***Benjamin Franklin***

Minimizing internal control failures

As we mentioned, control failures happen. We've already discussed how you can take steps to plan and prepare for them. But what's even better is taking active steps to minimize them.

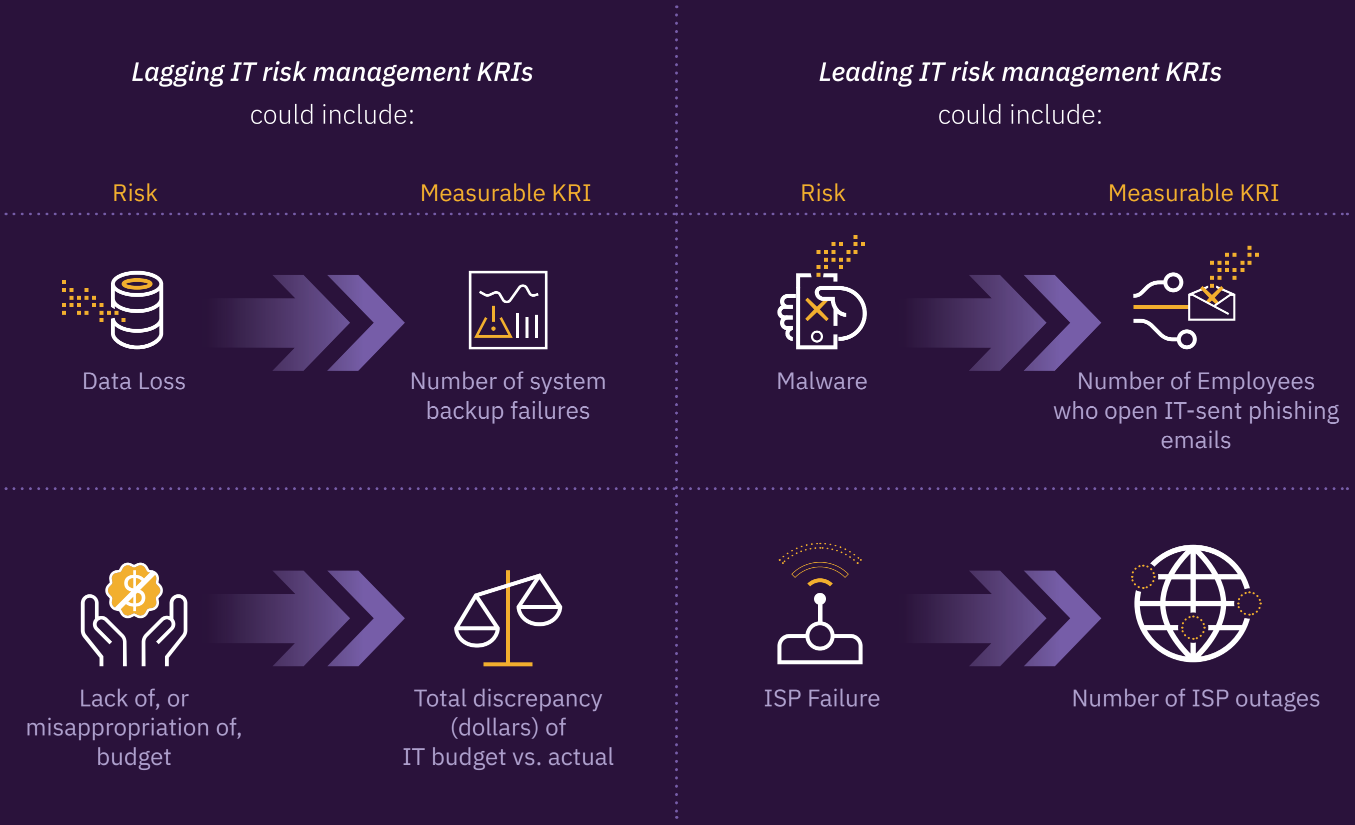
01

Monitor

Potential control failures can be monitored through key control effectiveness indicators (KCIs) or key risk indicators (KRIs). These are measurable ways to flag the possibility (leading KCI/KRI) of a failure, or the actual occurrence (lagging KCI/KRI) of a control failure.

You would construct these using existing and accessible data, then automate the monitoring so you'll be notified when they reach intolerable levels. You can also use a less-sophisticated manual process and spot-check your indicators, but this isn't as secure and could result in missed or overlooked failures.

FIGURE 2: EXAMPLES OF LAGGING & LEADING KRIs



Lagging IT risk management KRIs could include:

Risk	Measurable KRI
Data Loss	Number of system backup failures
Lack of, or misappropriation of, budget	Total discrepancy (dollars) of IT budget vs. actual

Leading IT risk management KRIs could include:

Risk	Measurable KRI
Malware	Number of Employees who open IT-sent phishing emails
ISP Failure	Number of ISP outages

02

Review & test

Controls can quickly become outdated and ineffective. To safeguard your organization, controls must be regularly reviewed and tested. Creating a schedule to review and test your controls is, as you may have guessed, a control in itself. Testing can be made easier through the use of automation. And while data automation is a lifesaver, it should (from time to time) be manually checked. On occasion, data connectors have failed or dirty data gets into the system, and this could mean you get incorrect test results.

Test the controls before and after deployment. This might be obvious, but it's very important. You've completed the risk assessment and designed the controls, now you'll need to test them to make sure they work as intended 100% of the time. And test the recovery plans, too. You will need a test plan so that all controls are tested periodically.

Testing and checking your contingency plan regularly isn't just a control—it's a good business practice.

CHECKLIST
Your recovery plan must:

- □ Be well-documented.
- □ Categorize and prioritize failures from low- to high-priority.
- □ Spell out what to do and who to contact in the event of a failure.
- □ Guide the specific action to be taken.
- □ Be regularly tested and reviewed.

BATTERIES
BATTERY
EMERGENCY
CANDLES
DISASTER PREPARATION LIST
• WATER
• NON-PERISHABLE FOOD
• BATTERY RADIO
• BATTERIES
• FIRST AID KIT
• FLASHLIGHT
• BLANKET
• CANDLES
• CAN OPENER
• PRESCRIPTION MEDS
• PET FOOD
• WARM CLOTHING
• CELL PHONE
• MATCHES
• WHISTLE
• CASH & KEYS
• HAND SANITIZER
• BASIC TOOL SET
• TRASH BAGS
• BABY SUPPLIES
• EMERGENCY CONTAC
• PERSONAL HYGIE
• DUST MASK
• IMPORTA
EMERGENCY INFORMATION
FIRST AID KIT
MATCHES

Welcome to internal controls utopia

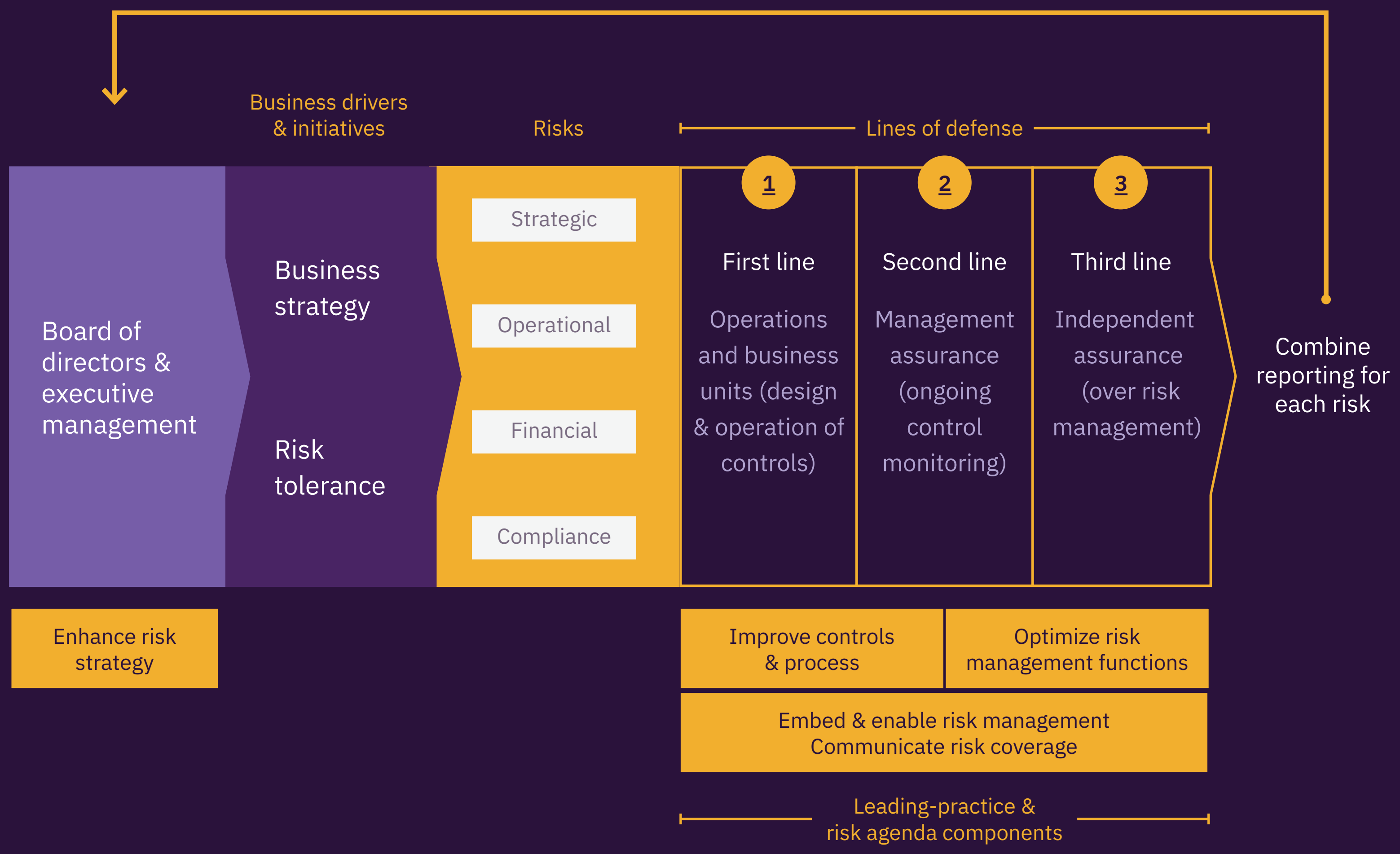
Congratulations, you've now reached internal controls utopia—a magical place where people, processes, and technology function in complete harmony.

- You have your controls, each department and individual understands the benefits of these controls, and they have put them in place within their own teams/functions.
- You review your controls to make sure they stay relevant.
- You continuously monitor your controls through connected data sources.
- You test and refine your controls on a regular basis.
- All of the controls across the organization are centrally itemized, prioritized, and managed.
- Automated reports and easily understood, self-serve dashboards create simple communication and real-time assurance report cards for auditors, the C-suite, and the board.
- Each control has a defined owner who actively participates in managing their controls.
- Notifications are automatically sent to control owners when KCI/KPI metrics begin to skew in an unfavorable direction.
- You've got a solid, regularly reviewed, and tested contingency plan in case of failure.

It's not an easy or short journey, but reaching this utopia is possible. In this ideal, yet realistic world, the entire organization works in chorus. The Three Lines of Defense have internal controls integrated into their day-to-day tasks, duplication is reduced, and everyone is able to work toward common objectives.

By centrally managing and introducing automation to control testing and workflows, assurance is improved and the workload can be more evenly distributed. Risk assurance is enhanced, compliance is achieved, and the C-suite and investors are more confident.

FIGURE 3: INTEGRATED RISK & CONTROL MODEL


Business drivers & initiatives
Risks
Lines of defense
Board of directors & executive management
Business strategy
Risk tolerance
Strategic
Operational
Financial
Compliance
1
First line
Operations and business units (design & operation of controls)
2
Second line
Management assurance (ongoing control monitoring)
3
Third line
Independent assurance (over risk management)
Combine reporting for each risk
Enhance risk strategy
Improve controls & process
Optimize risk management functions
Embed & enable risk management
Communicate risk coverage
Leading-practice & risk agenda components

In most organizations, almost all controls involve people, processes, and technology. And a well-designed internal control system is based on a sound risk assessment and management process that is reviewed and updated regularly. Our vision is to build an effective control system that is tried and tested and works predictably 100% of the time. What does your utopia look like?

The future of internal control

What does the future look like for internal control? Well, it's being shaped by the threats and vulnerabilities—and ultimately the risks—faced by organizations. This is why it's important to try to predict risks and initiate protective measures through controls.

Risk exposure is increasing thanks to new technology, the internet/connectivity, digitalization, and new ways of working. As connectivity and the reliance on the internet increases, weak controls in one's infrastructure could cripple entire organizations ... possibly even entire countries.

Technologies like machine learning, artificial intelligence, blockchain, global connectivity, wireless, and mobile platforms have introduced new dependencies. For example, block chain depends on multiple servers in different locations, usually in various countries, introducing increased geopolitical risk.

We work in a brave new world that includes almost total use of mobile devices, online transactions and banking, telecommuting, temporary project-based workforces, flexible hours, and outsourcing. All of these aspects make accountability difficult and all require appropriate and thorough controls to mitigate the inherent risk.

Add to that the trend to make things easier for us whenever we use tech (single sign-on, system user-id, and always signed-in apps) and one small opening/flaw in a system could lead to system-wide access.

Self-learning malicious software injected into a system would create havoc. We're already seeing viruses or bots that learn and change with their introduced environments. Controls, too, will need to be automated and self-learning to watch, learn, and predict potential threat behaviors.

So through the use of the same technologies that introduce risk, best practices, and a strategic approach, you can begin your journey toward your own internal controls utopia.

Further learning & resources

↳ ***IBM:*** *Global Threats Report*

↳ ***Ponemon Institute:*** *Cost of Insider Threats: Global*

↳ ***Accenture Security:*** *The cost of cybercrime*

↳ ***Ekran:*** *Insider Threat Statistics for 2019*

↳ ***Verizon:*** *DBIR Data Breaches Investigations Report 2019*

↳ ***PR Newswire :*** *Cyber attacks report*

↳ ***CyberCrime Magazine :*** *2019 Cybersecurity Almanac*

↳ ***Microsoft Corp :*** *2019 Global Cyber Risk Perception Survey*

↳ ***US General Accounting Office:*** *Internal Control Management and Evaluation Tool*

↳ ***Internal Audit 360 Internal Control Failures***

↳ ***CFO.Com:*** *Citigroup Internal Controls Failure*

↳ ***Harvard Law School:*** *Internal Control Failures*

↳ ***U.S. SEC:*** *SEC Charges The Hain Celestial Group with Internal Controls Failures*

↳ ***David Brewer:*** *Measuring effectiveness of an internal control system*

↳ ***ISACA:*** *Internal and Mitigating Control Selection*

Galvanize

ABOUT THE AUTHOR

Anil Jogani

Anil Jogani is a senior executive with considerable international experience in the IT industry throughout the UK, India, and Europe. A GRC, security, audit and ERP software solutions professional, Anil regularly presents at international events and writes on the topics of IT governance, security, data privacy, audit, and control.

ABOUT GALVANIZE

Galvanize delivers enterprise governance SaaS solutions that help governments and the world's largest companies quantify risk, stamp out fraud, and optimize performance.

wegalvanize.com

Our integrated family of products—including our cloud-based governance, risk management, and compliance (GRC) solution and flagship data analytics products—are used at all levels of the enterprise to help maximize growth opportunities by identifying and mitigating risk, protecting profits, and accelerating performance.