



**פּוּרְס**

# WELCOME

## בקרה פנימית ו-SOX בעולם הדיגיטל

SOX השלב הבא  
לאן מתקדמים מכאן? ואיך?



# Why do we need to consider changing our SOX program?

## Key drivers for change

Organizations should continually assess their SOX program with a focus on leveraging technology and automation to streamline activities and align the program with the company's strategic and compliance objectives.

The following are three key areas to consider when evaluating whether it's time to transform to your SOX program.

## Digital initiatives are picking up pace



- Is your organization adapting digital transformation?
- Is your SOX program keeping up with the fast pace of new technologies and the risks arising from them?
- Is your SOX program taking advantage of advances in technology to build even more intelligent, automated, efficient compliance programs?

## Pressure on cost is constant



- Many SOX programs remain heavily manual and costly, even after many years of SOX compliance.
- Do you know the total cost of your SOX program?
- Is the level of effort to execute SOX compliance activities distracting you from dedicating time to risks and activities directly tied to business objectives?

## The war for talent continues



- Is your organization experiencing higher turnover?
- Are you able to find the right resources in the market and retain those resources?
- Is your Internal Audit function looking to spend scarce resources on higher risk areas and to provide those resources with differentiated career opportunities?



Align objectives and use technology-enabled solutions within your SOX program to drive quality and balance cost while allowing internal resources to focus on higher risk, strategic activities.

# What does good look like? What are others doing?

## Target Operating Model:

**30%** Controls Tested using Automation, **40%** Controls Tested using Acceleration Centers, **30%** Core SOX Team



### Drive clear accountability

- Increase accountability in the first line.
- Deliver a competent, objective model that supports management's operating model and reliance objectives.
- Better deliver on a broad range of compliance obligations and other risk initiatives, including the Internal Audit mandate.



### Join the organization's digital transformation journey

- Assess the impact of intelligent automation adoption across different processes and controls and establish a framework that empowers a control mindset in the business.
- Share automation solutions with the business to support overall objectives.



### Find opportunities to continually enhance and optimize their SOX program

- Understand the total cost of compliance.
- Leverage results of a robust scoping and risk assessment to vary the nature, timing and extent (NTE) of management control testing and operating effectiveness assessments.
- Work with external auditors to understand the impact of auditor reliance on the overall SOX compliance strategy.
- Scale activities into other areas of integrated compliance to gain synergies and eliminate duplication of activities.
- Leverage flexible talent models.

# Take an objective look at SOX compliance within your organization—both the program and tactical delivery



## The Program

Every program should have a coordinated, agreed upon strategy to align stakeholders and ensure achievement of objectives. A strategy includes the following:

- ▶ **Vision and objectives**—A clear vision will help articulate what you want to achieve while defined objectives provide guidance to the rest of the program.
- ▶ **Operating model**—The operating model articulates ownership of the program, accountability for its various components and identifies integration points with other compliance initiatives.
- ▶ **Performance monitoring**—Align key performance indicators with objectives to determine when your program is on track and when adjustments need to be made.



## Tactical Delivery

Once the program has been calibrated, deep dive into tactical delivery to enable the function's ability to execute. Think through **what** you're delivering and revisit **how** you're delivering.

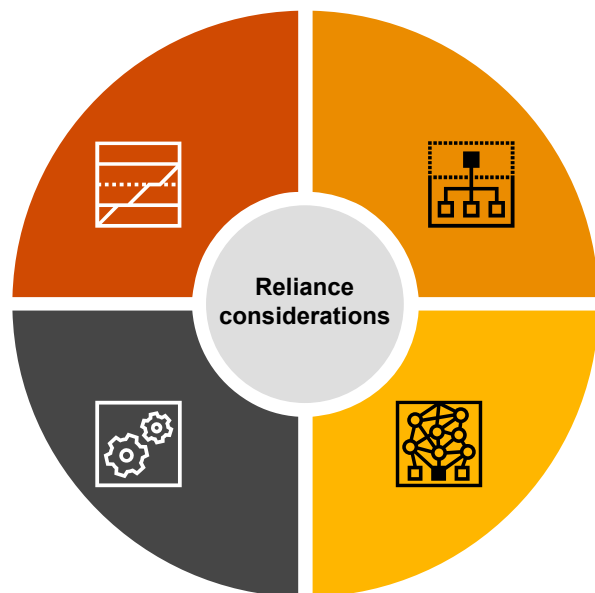
- ▶ **Focus effort in the right places**—A robust risk assessment and scoping exercise allows management to vary the nature, timing and extent (NTE) of testing and focus resources where it makes sense.
- ▶ **Reconsider your control set**—Controls change as the business changes and the reliance on technology increases. Your SOX program should have mechanisms to keep your internal control framework updated and pointed to the optimal set of controls.
- ▶ **Evaluate alternative methods**—Control testing may not be your only option. Use a combination of self assessments, data-enabled monitoring and emerging technologies (like RPA) for control testing to optimize the assessment process and provide earlier insights.



By focusing on these areas, we see opportunities to enhance efficiency, reduce disruption in the business, deliver incremental value from the process, and drive up to 30% out of the total cost of compliance.

# Finding the right reliance strategy

Organizations are taking a close look at their independent auditor reliance strategy. Reliance is an area where companies often spend considerable effort and resources with little visibility into the return on their investment. An understanding of the cost vs. benefit will help you calibrate program objectives and the way you assess your operating effectiveness.



## Walkthroughs

Are they necessary every year, and do your auditors rely on your control design assessments? If not, consider control self assessments.

## Reliance savings

Do you know what reliance is saving you? What does it cost you? Forcing yourself into a reliance model may not be worth it without transparency.

## Integration

Look across your organization— would it be as or more beneficial to integrate with other compliance efforts? You may create more synergies by focusing in house.

## Operating effectiveness

How are you getting comfort today? Management can look outside of sample based testing to provide greater assurance at lower cost.

Being deliberate about when and where reliance makes sense can help you:

- Reduce overall compliance costs
- Force transparency in ROI on reliance
- Balance level of effort with risk
- Consider other ways to assess your control environment
- Minimize disruption to you and the business
- Gain benefits from automation early

# What is your total cost of compliance?

While cost is usually not the sole driver for SOX decisions, it is an important factor when determining where and how to focus resources. Many companies do not have insight into the total cost of their SOX Program and would benefit from an exercise to understand it. We've outlined some sample costs to consider below.

SOX Lifecycle Component	Sample Cost Elements
Program management	<ul style="list-style-type: none"> <li>• Implement and maintain SOX policies and procedures</li> <li>• Administer quarterly certifications and sub-certifications</li> <li>• Facilitate coordination with management and other governance, risk and compliance functions across the SOX lifecycle as well as independent auditor</li> <li>• Report status and issues to stakeholders, including audit committee and executive reporting</li> </ul>
Risk assessment and scoping	<ul style="list-style-type: none"> <li>• Perform quarterly risk assessment and scoping analysis</li> <li>• Identify and map accounts, business processes, controls and IT assets</li> <li>• Validate scope with the business, stakeholders and independent auditors</li> </ul>
Control documentation & design	<ul style="list-style-type: none"> <li>• Perform walkthroughs and document processes, risks and controls</li> <li>• Perform design assessment</li> <li>• Validate accuracy of documentation and analysis with business</li> </ul>
Control testing & operating effectiveness	<ul style="list-style-type: none"> <li>• Control operation and documentation by management</li> <li>• Determine the control test plan, including nature, timing and extent of testing</li> <li>• Request evidence from the business and facilitate collection</li> <li>• Perform tests of operating effectiveness and relevant remediation testing</li> <li>• Document and validate results</li> </ul>
Evaluation & aggregation of deficiencies	<ul style="list-style-type: none"> <li>• Document control deficiencies</li> <li>• Report and validate deficiencies</li> <li>• Perform deficiency assessment and aggregation</li> </ul>

Cost-savings opportunities can be identified through:

- Communicating a clear vision and program objectives, ensuring alignment through delivery
- Focused, risk-based scoping
- Leveraging the most efficient testing techniques
- Being purposeful about your reliance approach
- Harnessing advanced technologies and data analytics to increase automation and efficiency
- Employing a flexible talent model to deliver SOX testing, enabling the ability to ramp up and down throughout the cycle



Understanding your Total Cost of Compliance supports your ability to make well-informed decisions about critical components of your program. Several key components include your approach to auditor reliance, your automation strategy and your operating model.

# Optimizing the control environment at all layers within Enterprise Systems landscape



## Enterprise Systems Security & Configuration - Native Automation

- Leverage the *capabilities of enterprise systems* to increase automation and maximize value



## GRC Technology

- Direct connect to enterprise systems to *automate monitoring* of configurations, security and transactions.
- Automate the workflow of compliance activities and *increase accountability and visibility* of compliance activities



## Automation & Analytics

- *Streamline performance and testing, and increase quality* in the controls environment through *purpose built* automations and analytics
- Leverage data visualization to *monitor testing* and *increase visibility* of compliance activities.



## Exception-based manual activities

- Some manual controls will continue to exist; where needed should be *efficient and effective*.



## Enterprise Systems Transformations

- Leading ERP systems
- Expanding the globalization of Enterprise Systems → Workday, Salesforce, etc.



## Governance Risk & Compliance Platforms

- SAP, Oracle, ERP Maestro, etc.
- Third party solutions (e.g., PwC Enterprise Control, Workiva, Archer, ServiceNow, etc.)



## Automation & Analytics

- Automation: UiPath, AA, Blue Prism, Alteryx
- Visualization: Tableau, Qlik, PowerBI
- Monitoring: PwC Enterprise Control

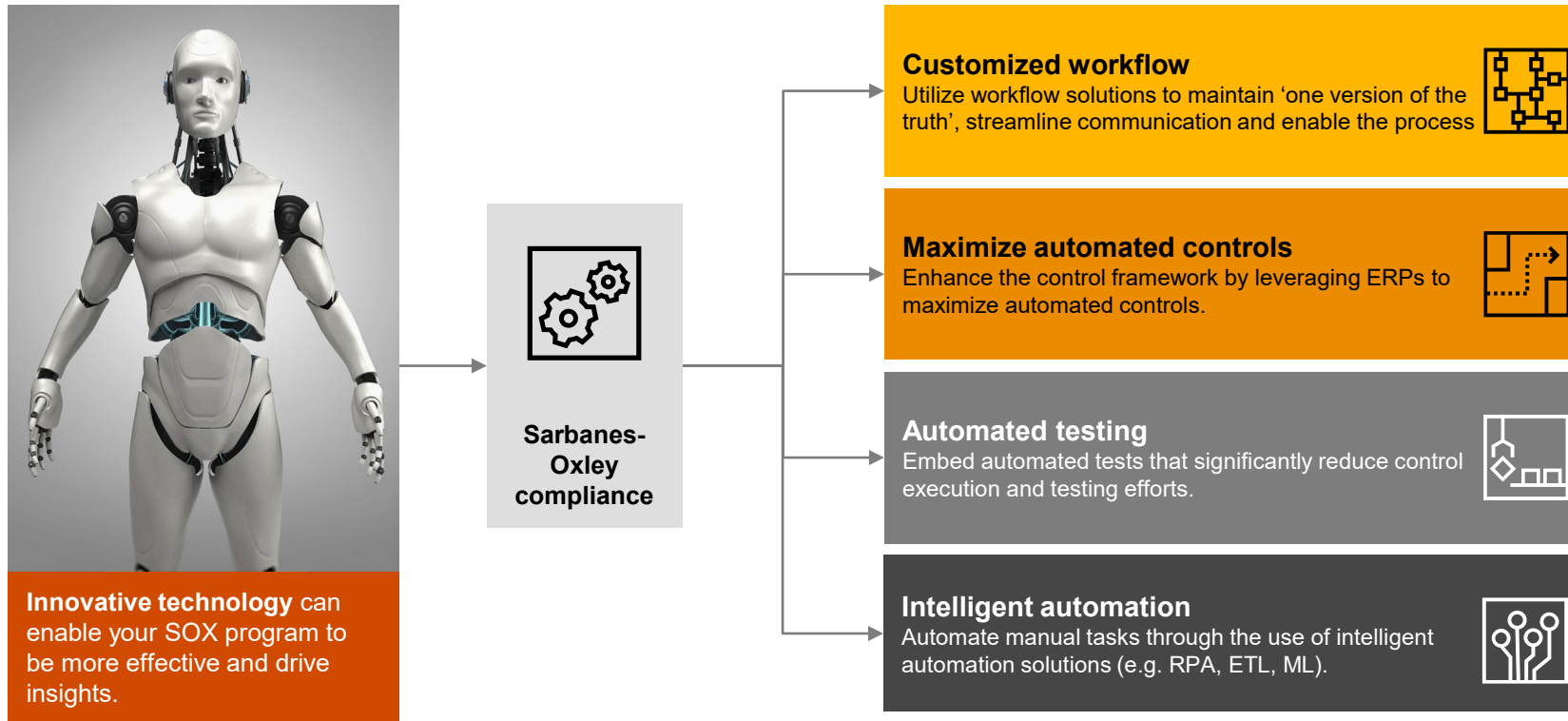


## Exception-based manual activities

- Human based controls leveraging traditional reports, paper based approvals, and review/reconciliation procedures.

# Harnessing automation in your program

Many organizations have innovation goals and automation is quickly becoming a “way of working”. When done “right” automation within your SOX program is powered by innovative technologies such as customized workflow, enhanced ERP functionalities and intelligent automation.



## Critical factors to consider:

- Be solution driven and tool agnostic
- Look at your end-to-end SOX program, not only control testing
- Consider piloting automation for quick wins, agility is key
- Demos are great, but focus on a scalable platform
- Remember -Digital transformation is a journey. As you standardize and optimize your environment, the greater the opportunity for automation and impact on total cost of compliance and quality.



Orchestrating bots, scripts and tools are critical to deploy a successful digital transformation strategy. Automation powered by a unique platform enables you to create a scalable environment that is more reliable and sustainable.



# Top 4 challenges for the next decade



## Automated working papers / testing

More tools will help us generate the SOX / controls testing procedures more effectively

01



## From Business Driven to Data Driven SOX

Data will be interfaced completely and directly to the auditors  
Controls will be designed more on data irregularities/errors and less on papers and manual testing procedures.

02



## From periodic to Continuous SOX monitoring

The testing procedures will run constantly instead of “testing phases / rounds”. This will also change the concept of having “internal testing” procedures before the auditors, as they will also have full visibility on your data and controls 24/7/365.

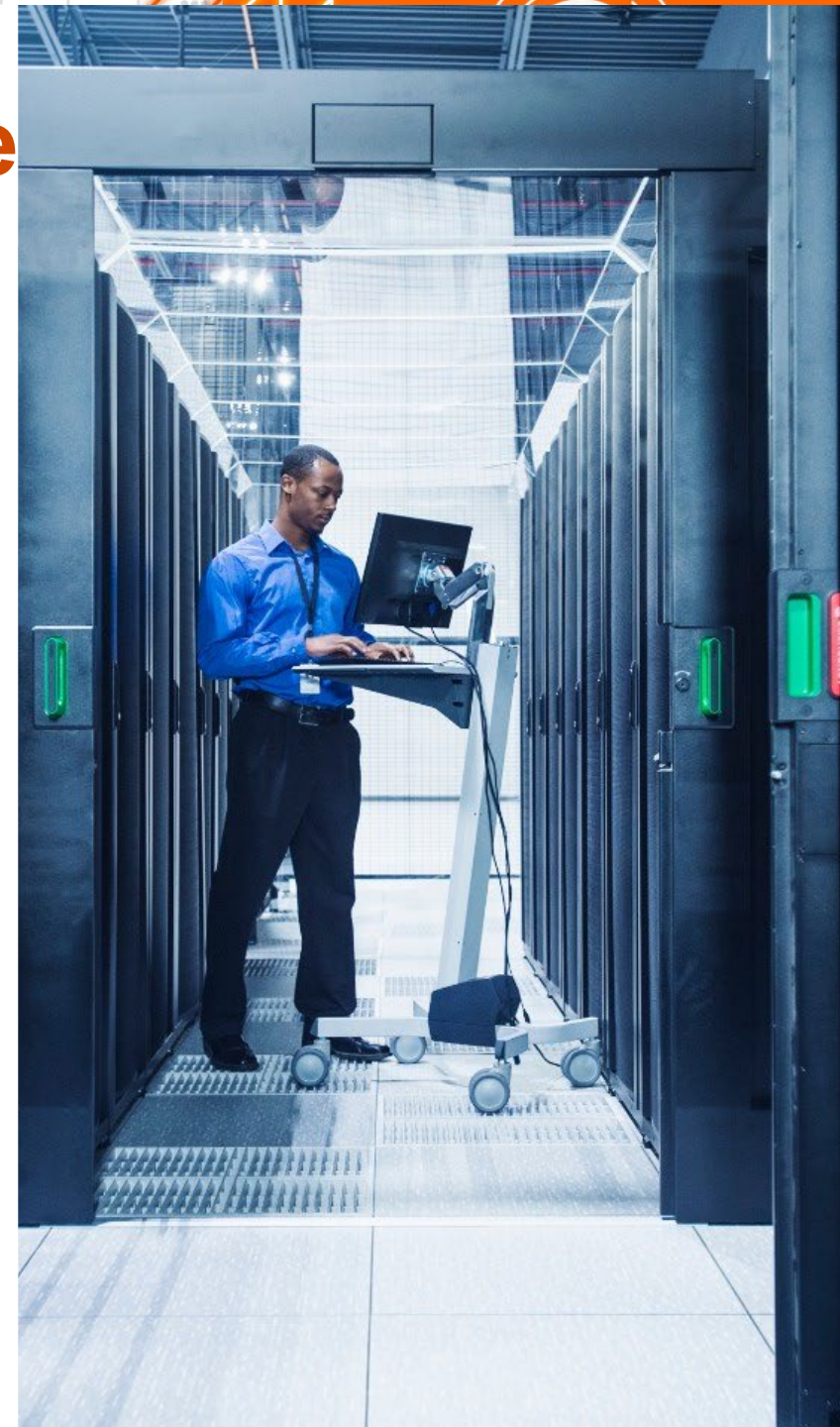
03



## From manual procedures through RPA to AI

We see more and more automated procedures run by robots. We will also see decision making by robots pretty soon. **Can we really test a review control operated by an intelligent robot?**

04



# What are the risks in using Chat GPT in business processes?

While Chat GPT can be a powerful tool for businesses, there are certainly risks to consider when using it in business processes. Some potential risks include:

- 1. Lack of control over output:** As a language model, Chat GPT generates responses based on patterns in the data it has been trained on. This means that the output may not always be accurate or appropriate for the situation. Additionally, because Chat GPT is constantly learning from new data, its output may change over time, making it difficult to maintain consistency.
- 2. Security concerns:** If sensitive information is shared through a Chat GPT-powered system, there is a risk that it could be accessed or intercepted by unauthorized parties. It's important to ensure that appropriate security measures are in place to protect data.
- 3. Legal and ethical considerations:** Depending on the nature of the business, there may be legal or ethical considerations to take into account when using Chat GPT. For example, if Chat GPT is used for customer service, there may be regulations around data privacy that need to be followed.
- 4. Dependence on technology:** Relying too heavily on Chat GPT-powered systems can create a risk of over-reliance on technology. If the system were to malfunction or be taken offline, it could cause disruptions to business processes.

To mitigate these risks, it's important to carefully consider the use cases for Chat GPT and implement appropriate safeguards and training for employees. Regularly testing and monitoring the system can also help identify and address any issues that arise.



pwc

# Thank you

**בקרה פנימית ו-SOX  
בעולם הדיגיטל**

Guy Sapir

PwC | Partner - Israel Risk Assurance Consulting  
Leader  
Office: +972-3-7954583 | Mobile: +972-54-5651291  
Email: [guy.sapir@pwc.com](mailto:guy.sapir@pwc.com)

