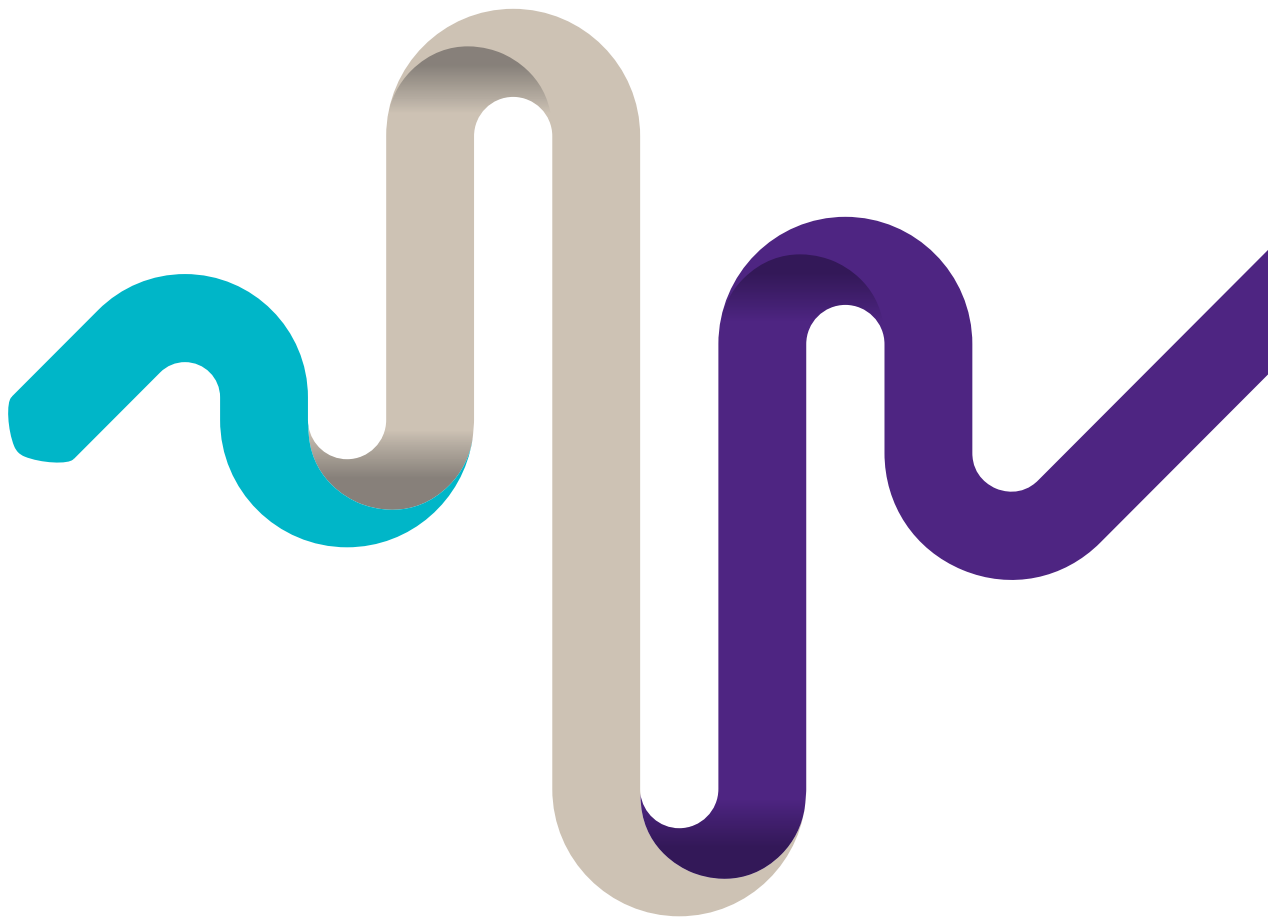



# UK SOX: Are you ready?





## As boards consider their readiness for UK SOX compliance there are a number of important practicalities to be thought about.

First and foremost is the need to critically assess the internal control environment and the means by which the board will gain assurance on the design and operating effectiveness of its internal financial controls to meet what is expected by the new regime.

The need to stand back and assess the effectiveness, efficiency and coverage of the internal control environment brings with it the need to also review technology controls underlying the systems that process and report financial data.

Notwithstanding the top down and bottom up control considerations, boards should also take a read of their culture and more specifically their risk culture and determine the need to reaffirm or recalibrate same so as to support and drive a more mature and embedded risk and control mind-set across the business going forward, again to be best placed to meet the expectations of the regime.

Given the extent of outsourcing and third party interaction inherent within business today assuring that the risk culture of third parties aligns to that of the business will remain critical. Boards need to have assurance that their business partners/ third parties internal control environments consistently meet their expectations. A worthwhile exercise in preparedness for UK SOX will be to assess the nature and extent of assurance the business currently gets on third party controls and the use of SOC reports to support the business's overall internal control mandate. Boards and management should agree a plan to have the necessary assurance mechanisms in situ.



**Sara McAllister**  
Partner,  
Business Risk Services  
T +353 (0)1 680 5716  
E [sara.mcallister@ie.gt.com](mailto:sara.mcallister@ie.gt.com)



# Internal controls framework

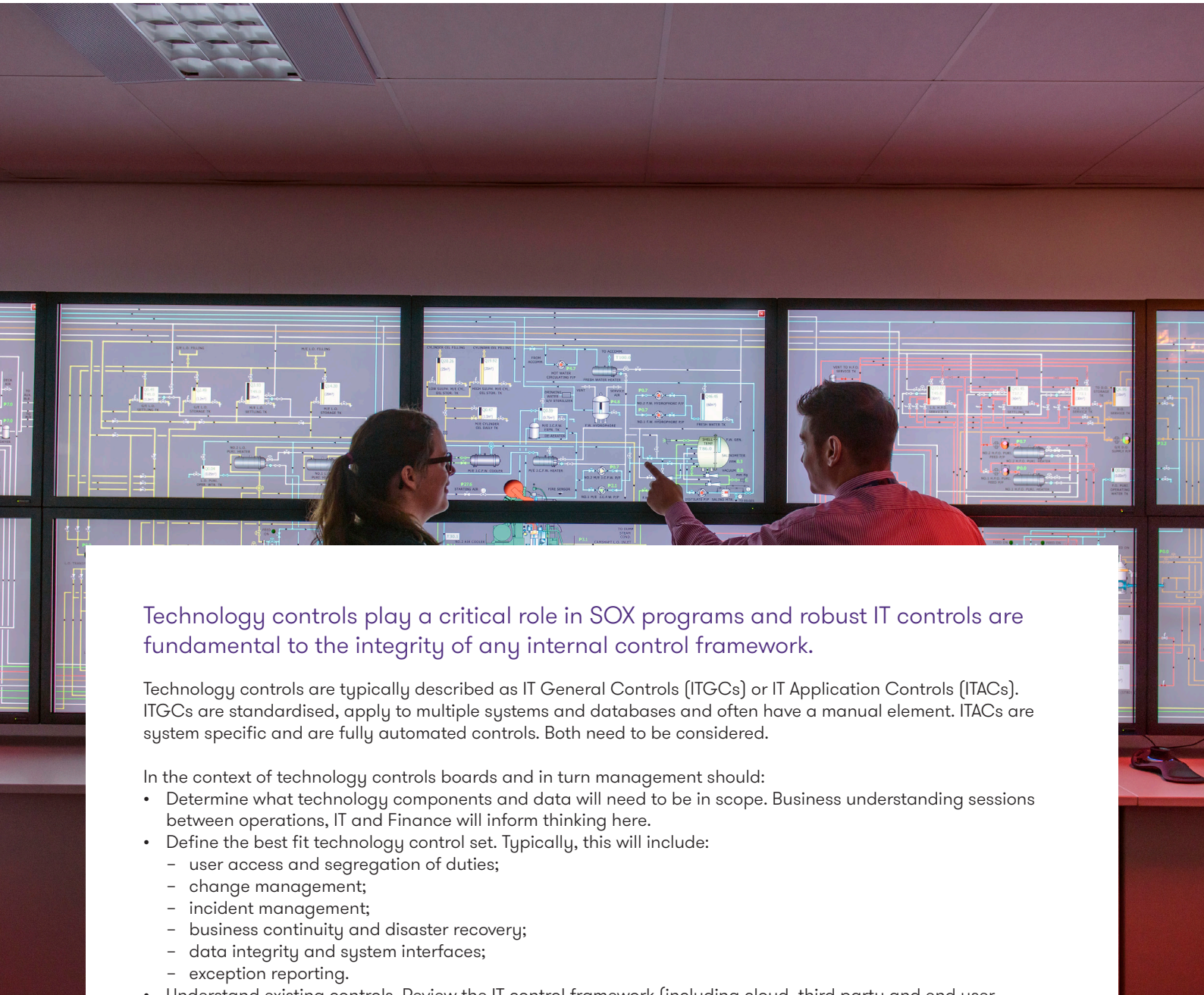


Most companies will have some form of an Internal Control Framework (ICF) in place but the extent to which it is right sized, embedded and adhered to will need to be revisited. As business operations evolve, so too should the underlying ICF.

Boards will need to work with their management team and advisors to address internal control priorities including:

- Aligning and revising financial controls to current financial processes.
- Allocating accountability/ownership for controls.
- Updating policies and procedures that govern said controls.
- Determining the optimum assurance mechanisms for testing and evidencing the design and operating effectiveness of internal controls. These may include involvement from internal finance teams, support from internal audit (in-house/co-source/outsource) and the use of certain self-assessment mechanisms. Most likely the answer will involve a mix of all three and will be fundamentally influenced by the risk maturity of the business.

# Technology controls



Technology controls play a critical role in SOX programs and robust IT controls are fundamental to the integrity of any internal control framework.

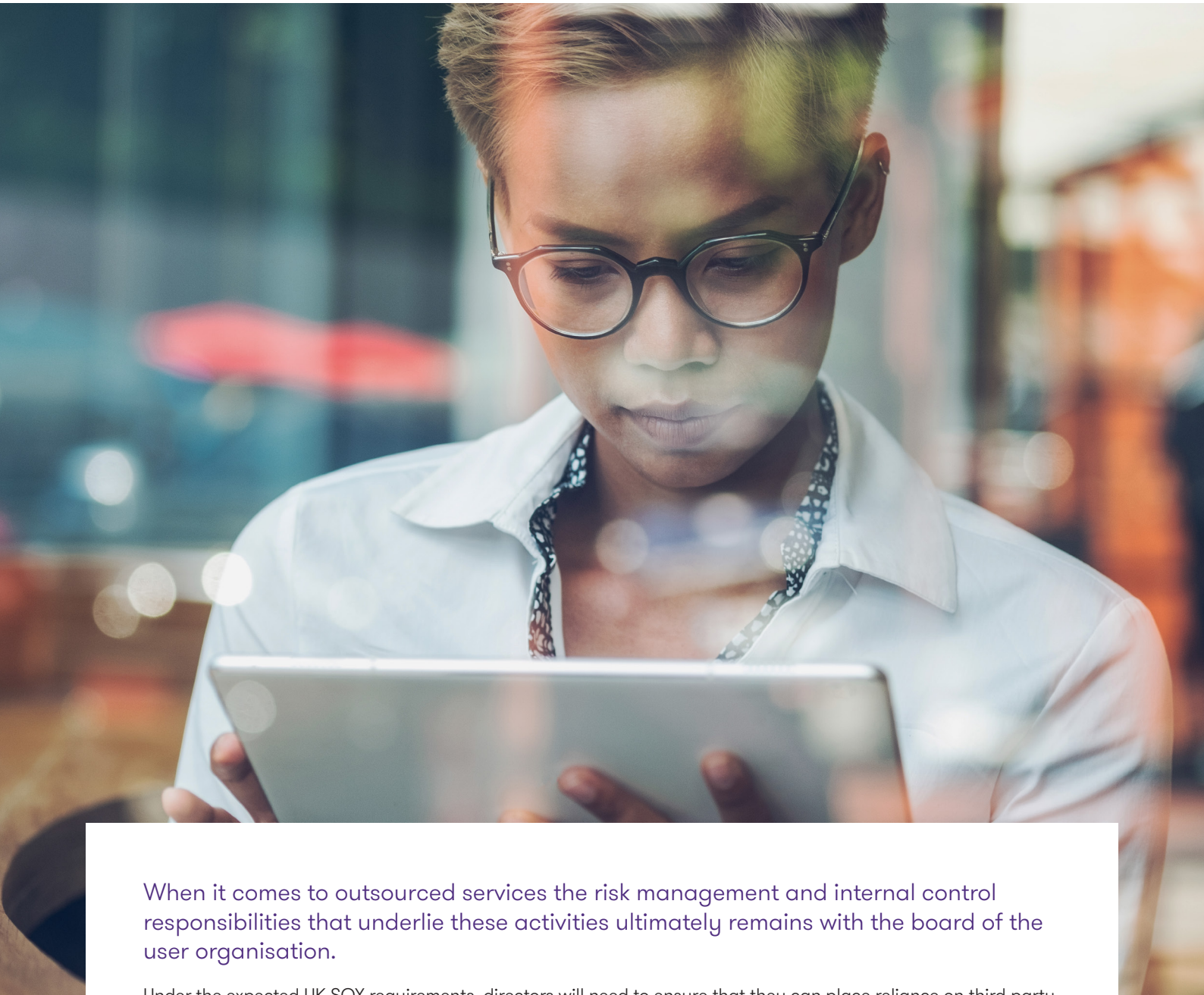
Technology controls are typically described as IT General Controls (ITGCs) or IT Application Controls (ITACs). ITGCs are standardised, apply to multiple systems and databases and often have a manual element. ITACs are system specific and are fully automated controls. Both need to be considered.

In the context of technology controls boards and in turn management should:

- Determine what technology components and data will need to be in scope. Business understanding sessions between operations, IT and Finance will inform thinking here.
- Define the best fit technology control set. Typically, this will include:
  - user access and segregation of duties;
  - change management;
  - incident management;
  - business continuity and disaster recovery;
  - data integrity and system interfaces;
  - exception reporting.
- Understand existing controls. Review the IT control framework (including cloud, third party and end user computing solution providers) that is in place across systems, applications and infrastructure to determine what needs to be enhanced and what can be leveraged.
- Review IT policies and procedures to determine validity, alignment and need for revision and ascertain levels of assurance and evidence currently in existence for said controls.
- Assess transparency and embeddedness of third party risk management practices.
- Compile a robust gap analysis and remediation plan.

Integrating efficiency into a technology controls framework is absolutely critical. Controls should be rationalised and optimised, wherever possible automated controls should be implemented and SOX implications should always be adequately considered at the outset of technology driven change and transformation projects.

# Third party assurance (SOC)



When it comes to outsourced services the risk management and internal control responsibilities that underlie these activities ultimately remains with the board of the user organisation.

Under the expected UK SOX requirements, directors will need to ensure that they can place reliance on third party organisation's internal control environments. A range of mechanisms can be used to varying degrees to gain this assurance and extent to which they are leveraged will depend on the number, scale and complexity of third party relationships in existence.

The deployment of a third party risk management framework in managing your end to end third party relationships from on-boarding to off-boarding provides a clear and transparent view of how third party risks are being monitored and actively managed by the business. The use of third party audits may also be valuable to augment in house monitoring and reporting activities. Alongside these tools is the use of SOC reports as mentioned above. Third parties find such mechanisms efficient as they can answer multiple customer concerns in respect of assuring financial controls (SOC1/ ISAE3402) and/ or technology controls (SOC2/ ISAE3000).

# Culture



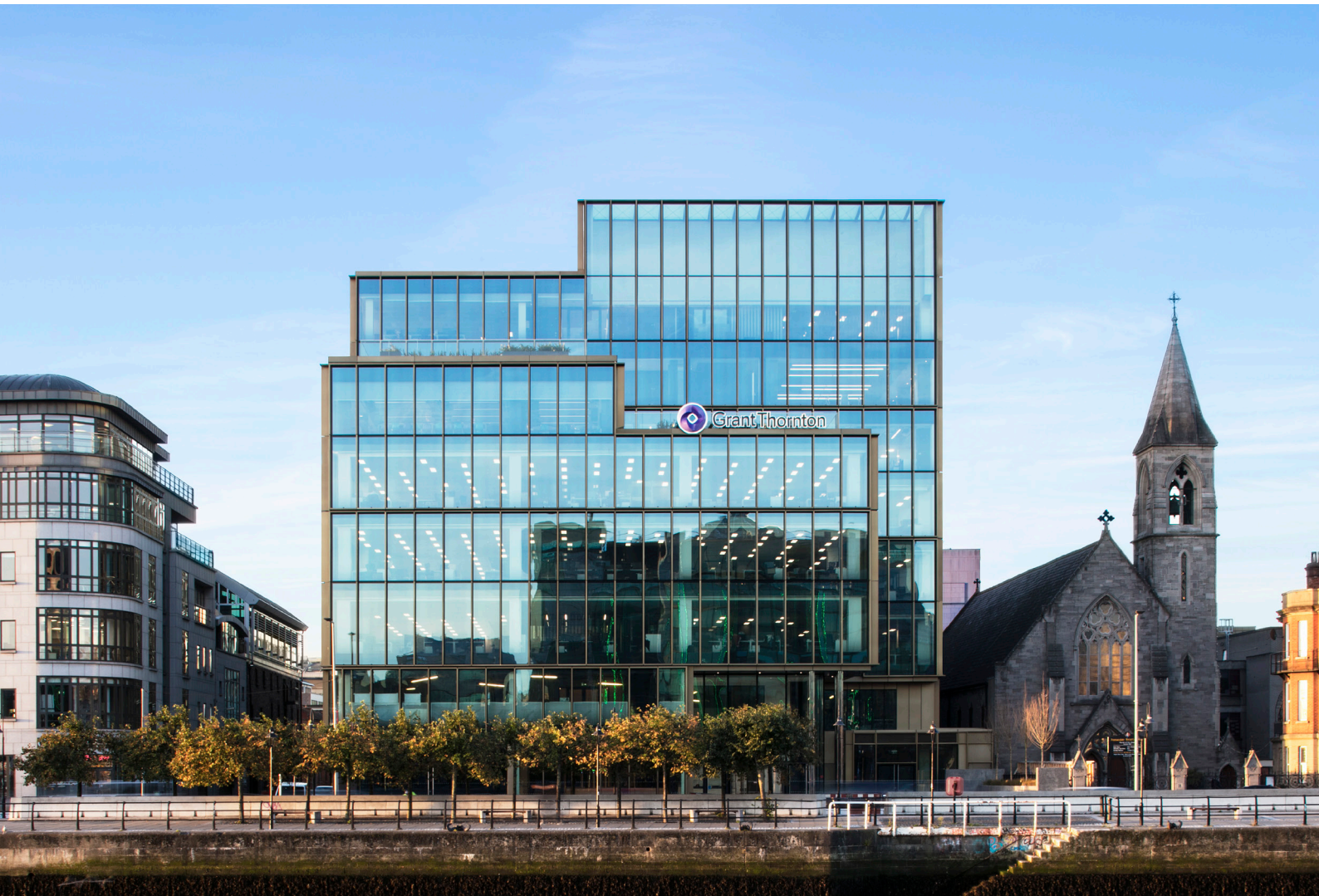
A business's underlying culture reflects the attitudes and behaviours of its management and employees. In that respect culture is fundamental to driving compliance with regimes like UK SOX.

A board will seek to:

- Develop/establish a culture that aligns to the new requirements. Embed that culture to ensure consistency and alignment in 'how things are done' so as to reduce risk.
- Link culture to strategy and in turn influence day to day decision making. Critical cultural success factors notably include:
  - **Leadership and accountability:** That being demonstrable and personal accountability for culture and behaviours at all levels supporting by regular and transparent communication.
  - **Objectives:** Performance management systems should mirror culture and expected attitudes and behaviours in respect of risk and control. Said recognition systems and promotions should foster strong role models.
  - **Learning and Development (L&D):** L&D programmes should be updated, including induction training to underpin and reaffirm cultural values.
  - **Embedding into core business activity:** Including procurement, projects, operations, risk, internal audit and board and management governance forums/ committees.
  - **Communication:** Finally, both internal and external communication teams need to reflect UK SOX requirements and any nuanced change of business values on the corporate website, intranet, and other forums.



# Contact us



Our BRS team can provide pragmatic advice on any or all of these considerations as you seek to plan your roadmap to meet the requirements of UK SOX.



**Sara McAllister**  
Partner,  
Business Risk Services  
T +353 (0)1 680 5716  
E [sara.mcallister@ie.gt.com](mailto:sara.mcallister@ie.gt.com)



**Onatkut Varis**  
Associate Director,  
Business Risk Services  
T +353 (0)1 680 5905  
E [onatkut.varis@ie.gt.com](mailto:onatkut.varis@ie.gt.com)



**Sean Quinn**  
Associate Director,  
Business Risk Services  
T +353 (0)1 433 2592  
E [sean.quinn@ie.gt.com](mailto:sean.quinn@ie.gt.com)



**Channele Da Silva**  
Manager,  
Business Risk Services  
T +353 (0)1 680 5852  
E [chanelle.dasilva@ie.gt.com](mailto:chanelle.dasilva@ie.gt.com)

Offices in Dublin, Belfast, Cork, Galway,  
Kildare, Limerick and Longford.

 [grantthornton.ie](https://www.grantthornton.ie)  [@GrantThorntonIE](https://twitter.com/GrantThorntonIE)  [Grant Thornton Ireland](https://www.linkedin.com/company/grant-thornton-ireland)



---

[grantthornton.ie](https://www.grantthornton.ie)

© 2021 Grant Thornton Ireland. All rights reserved. Authorised by Chartered Accountants Ireland ("CAI") to carry on investment business.

'Grant Thornton' refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more member firms, as the context requires. Grant Thornton International Ltd (GTIL) and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms. GTIL does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions. This publication has been prepared only as a guide. No responsibility can be accepted by us for loss occasioned to any person acting or refraining from acting as a result of any material in this publication.