Grant Thornton

An instinct for growth™

Technology risk services

Helping you meet your IT risk assurance and advisory requirements

January 2020

IT has been a key driver for success and operational efficiency in all industries. Innovations such as the use of social media, digital platforms, online services, cloud computing and virtualisation and new threats around data governance and cyber security have reinforced the importance of, and increased the risks associated with, the use of technology for our clients. Against the backdrop of new innovations, increasing regulatory burden and in the face of dynamic markets, tough competition, resource pressures and greater IT complexity, firms are facing increasing challenges to improve the performance and use of IT.

All of these factors heighten importance of that effective risk management, internal audit and corporate governance have to play in managing the risks associated with IT. This is where Grant Thornton's team of technology specialists can help, from the boardroom or the network, to IT strategy or system selection. This document highlights some of the IT related areas where we can help you manage your associated business risks.

Technology focus

Grant Thornton is one of the largest providers of professional services delivering assurance and advisory services to industries as diverse as financial services, telecoms, retail and the public sector, as well as small to medium sized enterprises (SMEs). Within technology risk services, our client service teams consist of highly specialised and experienced professionals with extensive experience of key risk management areas including:

- IT risk management
- Data and digital security
- Data governance
- Data analytics
- Business and IT resilience
- IT and business process outsourcing
- Project management
- IT operations
- Cyber security

Our specialist areas

We combine our deep technical skills and market understanding, with a desire to collaborate with you, to manage your IT and project risks.

We can support your requirements via co-source and outsource agreements or project specific engagements to suit your needs. This includes provision of resources in the following, but not limited to, specialist areas:

- IT internal audit
- Cyber security and privacy services
- Data analytics
- Business continuity and resilience
- Digital assurance advisory services
- Third party assurance
- Outsourcing risk management
- Project assurance and advisory services
- IT and Cyber due diligence

By developing an in-depth understanding of your business, we can effectively identify and assess IT risks and propose pragmatic solutions.

IT internal audit

Delivering your IT internal audit requirements

The role of internal audit is to provide assurance over the effectiveness of internal controls relied on by management. Internal audit helps an organisation achieve its objectives by systematically evaluating and improving the effectiveness of risk management and control processes. A strong IT audit capability is a critical component of any effective internal audit function.

We can help you fully assess the IT environments within your business and develop a robust IT audit plan that supports management, the audit committee and wider stakeholders.

We operate in line with the Chartered Institute of Internal Auditors'and ISACA's standards and can work with your internal audit function to provide specialist IT auditors, via outsourced or co-sourced arrangements. This is to help ensure IT risks are better identified, assessed and managed as appropriate for your business. Our IT specialists undertake:

- Integrated audits in conjunction with business auditors
- Business continuity
- Standalone specialist reviews in IT governance and strategy
- Digital audit, eg over the use of social media, web platforms, digital security and online journeys
- Application infrastructure and IT operational areas
- Data security and privacy audits
- Data analysis

We can also provide specialists with platform specific experience and practical knowledge of implementing good practice frameworks such as COBIT, ITIL and ISO 27001.

Case study

IT internal audit

Grant Thornton has provided outsourced and co-sourced internal audit services, including IT, to organisations of all sizes.

For one blue chip banking client, we have, over the last few years, supplemented their existing internal audit team as and when required. We have provided IT auditors in the following areas:

- Technical infrastructure
- Third party risk reviews
- Cyber security
- Application reviews
- Programme assurance
- Payments certifications and application infrastructure audits
- Integrated audits with the business auditors
- IT operational and audit planning activities.
- Performed fraud risk assessment and payroll IT controls reviews to address specific issues identified

These resources were provided to meet specialist requirements, cover for leavers or maternity leave and to offer support in unforeseen circumstances.

COBIT – Control Objectives for Information and Related Technology
ITIL – Information Technology Infrastructure Library
ISO 27001 – Information Security Standard

Cyber security and privacy services

Case study

Working with you to protect your organisation from cyber security threats and data theft

The need for reliable and up to date security practices, supported by the development of a mature organisation wide security culture, where your staff become part of the solution, is now critical to protect organisational interests and executive reputations.

We have a team of cyber security and privacy professionals who have performed many reviews including:

- Security vulnerability assessments and health checks
- Compliance with legislation such as GDPR or frameworks such as ISO 27001 / ISO 27701
- Cyber health-check
- Cyber crime incident response and investigation
- In-depth analysis and benchmarking of the maturity of the security culture across a firm including information security governance reviews
- Third party security risk assessments
- Penetration Testing, Hacking Services, Red-Teaming
- Digital Forensics services
- Payment security (PCI-DSS, SWIFT-payments)
- Identity and access management
- Cyber and Data Privacy Awareness training program

Cyber security

Our client, an e-wallet provider asked, asked us to perform a company-wide assessment of the effectiveness of their information security operating model and privacy governance framework. Through interviews with key staff and assessment of policies and tools in operation, including incident management including management procedures, we were able to identify a good practice practical information security and Data Protection operating model. We also identified a number of recommendations for enhancing the effectiveness of the client's information security and Data Privacy operations.

Data analytics

Helping you realise the value of your data

As part of internal audit assignments and/or one-off reviews we have undertaken numerous engagements, using Computer Assisted Audit Techniques (CAATs) to help our clients analyse the details behind their data. We can provide customised data services including the following:

- Data forensics – detailed analysis and mining of information
- Financial analysis – for example identification of anomalies in accounts payable/accounts receivable
- Fraud analytics
- Payroll – identification of ghost employees, duplicate payments
- Tax data analysis using proprietary data scripts
- Regulatory analytics, eg anti-money laundering, know your customer, solvency II, market abuse, transaction reporting
- Data model analytics

Case study

Data analytics

A leading payroll service provider wanted to upgrade their 'mission critical' systems but knew that they had legacy data issues to resolve. We reviewed three years' worth of transactional accounting data using our data analytical software skills. We matched over one billion pounds worth of data, contained within over 100 million records, to identify differences between the key business database and the financial accounting system. The results were analysed, accounting differences and the reason for errors identified and remedial steps implemented. This allowed effective migration to new systems.

Digital assurance and advisory services

Case study

Connected, online, mobile or social media activities are an inherent part of our lives. The way we communicate, obtain and share information has changed, and along with that, our buying habits and expectations have changed. We Google more, trust customer reviews and expect next day delivery. This change in behaviour may seem superficial, but it has fundamental implications for a business trying to meet or exceed these customer expectations. 'Digital', often used to refer to online, mobile, cloud, or social technology, is not just a technology or a channel problem; it permeates the fabric of what we know as business today.

The digital platforms not only provide vast new opportunities, but also introduce risks relating to data and information security, infrastructure resilience and operational availability.

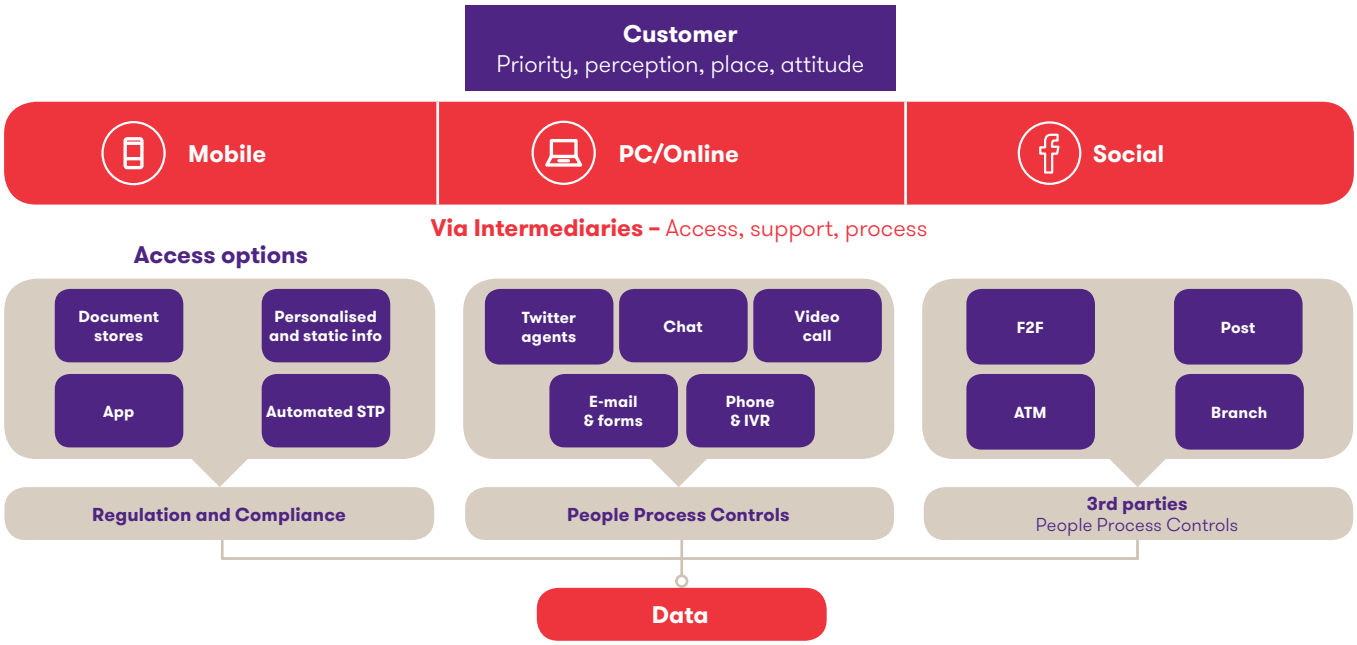
We can help you manage your digital risks associated with:

- Digital security
- Use of social media
- E-commerce gateways and interfaces
- Online service portals
- Third party service providers
- Use of mobile devices
- Data governance and risk management

Digital strategy/social media review

We delivered a digital strategy review to a world class conference centre company who were challenging the way they operated. They wanted to reach out to their customers and maintain contact with their repeat attendees. Our digital experts identified, through a review of their social media approach, that they needed to think about the customer experience and how social media made a huge impact on the touch points with their customer base. We gave them techniques to use to create an experience that stayed in the memory of this customer base. We looked at the risks associated with social media and digital implementation so that, whilst delivering these techniques they didn't expose the business to inappropriate risk.

Digital communication is now a norm for doing business



Business resilience

Does your organisation have the resilience to stand up to a high profile incident?

Business resilience is the ability of an organisation to minimise disruption and be able to function during an incident. It covers all aspects of business continuity, technology disaster recovery, incident management and financial resilience.

Business resilience is pivotal to maintaining business activities in the modern age of inter-connected global operations, just in time production and complex operational relationships. Maintaining your reputation and delivering on time are fundamental to all professional relationships.

Organisations need to anticipate and have proven strategies to effectively respond to disruptive events, maintain critical operations and learn from events to better prepare for future challenges.

By partnering with organisations and using our wealth of experience, we can better prepare organisations to face the challenges that these disruptive events create. Our business resilience specialists can offer support in the following areas:

- Crisis management
- Incident management
- Cyber resilience
- Business continuity
- Disaster recovery
- IT resilience

Industry guidance

Our business resilience services are based on the guidance contained in relevant British and international standards, including:

BS 11200	BS 65000	ISO 22301	ISO 22313
Crisis management: guidance to good practice	Organisational resilience: guidance	Business continuity management systems: requirements	Business continuity management systems: guidance

Case study

Business resilience

Grant Thornton supported a FTSE 250 construction firm in assessing and reporting on the level of resilience in the organisation and provide recommendations for any potential improvements and efficiencies.

Using a hybrid approach of documentary review, onsite inspections, evidence gathering interviews from key stakeholders, we benchmarked the client's resilience against industry good practice, the relevant British Standard BS 65000:2014 Guidance on organizational resilience and Grant Thornton intellectual property. We identified tactical and strategic improvement opportunities to the resilience programme, relating to programme efficiencies and risk management enhancements and were able to help develop a standardised approach across the organisation.

Third party assurance

Outsourcing a service to a third party does not outsource responsibility

The growing diversity of third party service providers has increased the breadth of a company's footprint but has also introduced new risks. Third party service providers can range from traditional outsourcing of IT and payroll and financial processing to newer services such as web hosting and cloud computing.

All third party agreements introduce new risks. We can help you manage these by:

- Delivering independent assurance over outsourcing programmes/projects
- Assessing the effectiveness of service level monitoring and third party cost verification
- Providing service auditor reports. These give operational assurance over third party services, using established standards such as AAF 01/06, ISAE 3402 / 3000, SSAE 16 (previously SAS 70), and ITF 01/07.

Our IT specialists have cross market experience covering all industries including financial services, retail, telecommunications and the public sector. We are confident that we can get the right combination of technology, engagement and industry experience to meet your IT risk management needs.

Case study

Third party assurance

Grant Thornton has helped many clients in obtaining service auditor reports against the AAF, ISAE3402 / 3000 and SSAE 16 frameworks.

For one client we initially held communications/understanding workshops to enhance awareness and communicate the implications of a service auditor report. We then facilitated identification of in-scope control objectives and associated control activities before performing a gap analysis. We have subsequently completed a number of type 1 and type 2 AAF reports in different parts of the client's business.

AAF 01/06
Audit and Assurance Faculty of ICAEW 01/06

ISAE 3402
International Standards for Assurance Engagements 3402

SSAE 16
Statement on Standards for Attestation Engagements 16

SAS 70
Service Organisation Auditing Standards 70

ITF 01/07
Information Technology Faculty of ICAEW 01/07

Outsourcing risk management

Third party risk management activities are a key means for managing a company's exposure arising from their service providers and business partners

Third party process risk management

There are many risks associated with use of third parties in financial, regulatory and operational terms. Whilst processes and services can be outsourced or shared, each organisation still owns the ultimate responsibility for their organisation's risks, emanating from those activities.

Many organisations are now using third parties to provide functions that were previously deemed to be core activities. This can be a cost effective and efficient strategy, but it can also add a considerable degree of complexity to the design and implementation of the appropriate governance, risk and controls framework.

In addition to the relevant local regulatory requirements other international regulators' requirements may also need to be considered. The subsequent challenges for global firms can be complex and considerable when designing a framework that is fit for purpose across a diverse portfolio of regulatory jurisdictions.

We have a team of risk management specialists who have undertaken various third party risk management reviews of outsourcing projects and operational contracts, and who have helped to identify operational risks and improvement opportunities. We have performed the following third party risk management reviews:

- Risk reviews of IT outsourcing projects
- Reviews over vendor management and governance
- Third party functional and IT performance audits
- Third party business resilience reviews

Case study

Cloud computing

We were engaged to help the internal audit department of a leading utility company to identify weaknesses in the company controls for their cloud service providers. We created a tailored set of questionnaires according to the established cloud service model, (software, platform or infrastructure as a service). We identified a large sample of cloud providers available in the market and benchmarked them against the list of suppliers listed in purchase orders raised. This allowed us to identify cloud solutions that the IT department was not aware of.

Additionally, a review of contracts for selected providers was performed and we were able to identify weaknesses in the contract designs. A lack of definition on the minimum requirements for cloud solutions led to contract agreements with no standardisation on the minimum controls that the provider needed to comply with.

Project assurance and advisory services

Applying industry standards and best practices, combined with practical experience, to minimise the risk of project failure

Our project risk management specialists have a wealth of cross industry project management and project assurance expertise that can help our clients' transformation projects throughout the project lifecycle; from project initiation through to post implementation. Areas in which we have provided clients with assurance or project support include:

- Programme/project frameworks for managing substantial change
- Programmes and system development governance review
- Systems specification selection and implementation
- Project gateway reviews
- Pre-go live review
- Post-implementation reviews
- Project risk reviews
- Project critical friend

Case study

Project assurance and advisory services

Grant Thornton was engaged to review the lifecycle of a major business transformation programme within a large multi-national investment management firm. The core business objective was to redefine the firm's complex functional operating model in order to provide integrated and simplified processes and fit for purpose systems.

Enhanced processes and capability were delivered to front, middle and back office services which allowed the firm to meet their on-going risk and the regulatory requirements. This included compliance with Capital Requirements Directive IV (CRD IV) and Foreign Account Tax Compliance Act (FATCA).

Grant Thornton also delivered independent project review audits, providing management with an understanding of the risks associated with the overall project planning/design, functional testing, acceptance testing and technology and business parallel runs before 'go live'.

IT and Cyber due diligence

Technology is a key enabler for many organisations today and this can be enhanced as a result of mergers or acquisitions

Products and services are often integrated with associated applications and systems. It is therefore very important, when executing effective IT due diligence, to identify IT synergies and risks as part of the transaction.

Our specialist team works with the buyer and target organisation to establish the benefits and risks related to the technology environment as part of the proposed transaction. IT assets, contracts, business processes and products or lines of business are analysed to understand the potential risks and impact of these on future cash flow and may include:

- Consolidation plans for business processes, applications and technical infrastructure
- IT organisational structure and the impact of proposed changes
- Network, application and information architecture
- Data centres, premises and facilities
- Contracts with staff, vendors, partners, customers and business process service providers
- Technology directions and trends
- Feasibility studies and reality checks performed
- Enterprise position on risk, time-to-market and IT quality requirements

Case study

IT due diligence

A large insurance company was undertaking due diligence over a medical assist business that serviced tourists on holidays abroad.

As part of a broader buy side engagement, our IT due diligence team completed an assessment of integration risks to confirm that the acquisition technology environment was fit for purpose and aligned to the acquirer IT environment. We performed technology risk assessments over applications, the infrastructure, operations and people.

We identified risks relating to cyber, third party contractual arrangements that the target was tied into which could potentially cause unexpected costs and operational problems for our client after the acquisition. We also identified licensing implications associated with hardware and software that would have significant cost implications if the target was acquired. As well as identifying several technology integration risks, our report highlighted a variety of concerns that played a material impact on the offer price for the medical assist business that was made.

Why Grant Thornton?

Our team has experience of undertaking significant IT assurance and advisory engagements, within professional services that is supplemented with real industry experience. We have developed a team of specialists in IT audit, cybersecurity, data, project and third party assurance. We have worked with organisations of all sizes across all industries and can tailor our services to meet client needs. Our assistance can range from providing a single additional expert resource to supplementing an internal IT function or to providing a completely outsourced service for the provision and support of audit or consulting services.

We understand your business. Commercially minded and risk focused, our team of independent thinkers offers, we believe, the best combination of quality, expertise and value. We aim to work in partnership with you to deliver incisive, value-adding results. Our team features experienced audit and risk experts, who have held senior positions in leading organisations. We have considerable experience of providing these services in the financial services, corporate and public sectors.

For further information, please contact:

Christos Makedonas
Managing Director
Technology Risk Services
T +357 22600000
E Christos.Makedonas@cy.gt.com

Grant Thornton
An instinct for growth™

grantthornton.com.cy