Kevane Grant Thornton
An instinct for growth™

Kevane Grant Thornton LLP
33 Bolivia Street
Suite 400
San Juan, PR 00917-2013

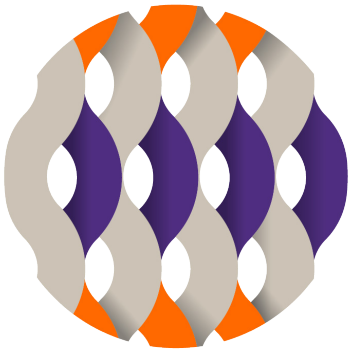
T + 1 787 754 1915

F + 1 787 751 1284

E kgt@pr.gt.com

linkedin.com/company/kevane-grant-thornton
facebook.com/kevanegrantthornton

Kevane Grant Thornton Mailbag



25 May 2017 | Issue 74

Dear clients and friends:

The Kevane Grant Thornton Mailbag is your link to all our communications related to the operations of businesses in Puerto Rico. Our purpose is to offer you with up-to-date information concerning audit, tax, advisory and accounting matters that might have an impact on individuals or in the way you conduct your business in Puerto Rico.

All our previous Alerts publications can be accessed in our webpage or you can also receive them by downloading our business and tax mobile application for free through the App Store or Google Play. We welcome your feedback at kgt@pr.gt.com

View our monthly publications below

Kevane Grant Thornton

An instinct for growth™

Audit Alert: AICPA introduces cybersecurity risk management reporting framework

Aida Ramirez
Partner Head of Audit
Kevane Grant Thornton
T (1) 787 754 1915
E aida.ramirez@pr.gt.com

Call to action
Access our Monthly Alerts on:
www.grantthornton.pr

The AICPA introduced a new cybersecurity risk management reporting framework, which will create a common language that can be used to communicate about, and report on, cybersecurity risk management efforts

The framework suggests the need for three key pieces of cybersecurity information:

- Management's description of the organization's cybersecurity risk management program
- Management's assertion about the program description and the effectiveness of the controls within that program
- The CPA's opinion about the description and control effectiveness

Two sets of criteria were issued to support this new framework:

- Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program – Criteria to be used by management when describing cybersecurity risk management programs and by CPAs in their evaluation of management's description
- 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy – Criteria for the security, availability, and confidentiality for use by management and CPAs when evaluating the effectiveness of the controls in the cybersecurity risk management program in achieving the cybersecurity objectives

An attest guide, "Reporting on an Entity's Cybersecurity Risk Management Program and Controls," will be published in the near future to assist CPAs engaged to examine and report on an entity's cybersecurity risk management program.

Source: Grant Thornton, *On the Horizon*, May 4, 2017.

We are committed to keep you updated of all developments that may affect the way you do business in Puerto Rico. Please contact us for further assistance in relation to this or any other matter.

Kevane Grant Thornton

An instinct for growth™

Kevane Grant Thornton
An instinct for growth™

Tax Alert: Comparison of Federal Tax Reform proposals

Information as of May 15, 2017

On April 26, 2017, President Donald J. Trump announced his proposed 2017 Tax Reform for Economic Growth and American Jobs, which calls for lower individual tax brackets, the doubling of the standard deduction, the repeal of both the alternative minimum tax and the estate tax, and the expansion of child tax credits and dependent care expenses. It also proposes lowering the business tax rates to 15%. The reform also calls for the US to transition from its current worldwide tax system to a territorial tax system, and for the enactment of a one-time repatriation tax on the foreign earnings of US companies. On the other hand, the Republicans have issued their proposed tax plan known as "A Better Way" tax reform blueprint.

The following table intends to compare the guidelines under both tax reform proposals.

Proposed US Tax Reform

Topic	Trump Administration	House Blueprint	Comments
Individual income tax rates	10%, 25% and 35%	0, 12%, 25%, 33%	The filing status for 2017 will continue to be: (i) married filing jointly, (ii) head of household, (iii) unmarried individuals (other than surviving spouses and heads of households) and (iv) married individuals filing separate returns.
Standard deduction	Double the current standard deduction: $12,700 for single individuals; $18,700 for head of household; $25,400 for single taxpayers.	$12,000 for single individuals; $18,000 for single individuals with a child in the household; $24,000 for married filing jointly.	Both proposals are intending to double the standard deduction by the individual filing status.
Itemized deductions	Maintain charitable contribution and mortgage interest deductions.	Eliminates all itemized deductions except mortgage interest deduction and the charitable contribution deduction.	Basically, the same under both proposals.
AMT (Individual)	Repeal.	Repeal.	
Child-related expenses	Tax relief for families with child and dependent care expenses. Details not specifically addressed.	$1,500 credit (consolidates child credit and personal exemption for dependents); first $1,000 refundable as under current law. Phase-out credit to begin at $150,000 for married filing jointly.	Under the tax reform blueprint, the marriage penalty tax that exists in the current-law phase-out of the child credit will be eliminated, so that married couples will be able to earn up to $150,000 before their child credits start phasing out.
Net Investment Income Tax	Repeal.	Repeal.	
Corporate Tax Rates	15% business tax rate.	20% flat rate.	Both proposals consider a reduction in corporate tax rates.
AMT (Corporate)	Repeal.	Repeal.	

Business Deductions/Credits	Eliminate tax breaks for special interests.	Full and immediate write-off of business. investment for both tangible and intangible assets (eliminates depreciation).	The Blueprint will provide business with the benefit of fully and immediately. writing off (or "expensing") the cost of investments.
Tax Rate on Pass-through Entities	15% business tax rate.	Maximum rate of 25% on income earned from small businesses and pass-through entities. Deduction allowed for reasonable compensation paid to owner-operator.	The 33/35% bracket will not apply to active business income of sole proprietorships and pass through entities. Sole proprietorships and pass-through businesses will pay or be treated as having paid reasonable compensation to their owner-operators. Such compensation will be deductible by the business and will be subject to tax at the graduated rates for families and individuals.
Estate Tax	Repeal.	Repeal.	
Imports and Exports	Not specifically addressed.	Exempting exports and taxing imports. Products, services and intangibles that are (1) exported from the United States will not be subject to US tax regardless of where they are produced; and (2) sold into the United States will be subject to US tax regardless where they are produced.	The blueprint eliminates the existing self-imposed export penalty and import subsidy by moving to a destination-basis tax system. Under a destination-basis approach, tax jurisdiction follows the location of consumption rather than the location of production. In addition, border adjustments mean that it does not matter where a company is incorporated; sales to US customers are taxed and sales to foreign customers are exempt; regardless of whether the taxpayer is foreign or domestic.
Taxation of Foreign Income (Business Income)	Territorial tax system	Territorial tax system; active business income (products, services and intangibles sold outside the United States) will not be subject to US tax.	Under the blueprint proposal, products, services and intangibles that are exported outside the United States will not be subject to US tax regardless where they are produced. It also means that products, services and intangibles that are imported into the United States will be subject to US tax regardless of where they are produced.

Taxation of Foreign Income (Investment or Passive Income)	**Territorial tax system.**	**100% exemption for dividends from foreign subsidiaries.**	**This will allow US-based companies to compete in global markets, and bring to the US their foreign earnings in order to be reinvested in the US.**
Anti-deferral (Repatriation Tax)	One-time tax on money held overseas. Rate not specifically addressed.	8.75% rate for accumulated foreign earnings held in cash or cash equivalents; 3.5% rate for other earnings. Liability paid over 8-year period.	The Blueprint proposes to provide rules that will allow foreign earnings that have accumulated overseas under the old system to be brought to the United States.
Anti-deferral (Ongoing Income of Foreign Subsidiaries)	Not specifically addressed.	Bulk of Subpart F rules repealed.	The blueprint will allow the subpart F rules of the current international tax regime, which are some of the most complex rules in the tax code, to be significantly streamlined and simplified.

Please contact our Tax Department should additional information is required regarding this or any other tax issue. We will be glad to assist you.

María de los Angeles Rivera
Partner Head of Tax and
IBC Director
Kevane Grant Thornton
E maria.rivera@pr.gt.com

Lina Morales
Tax Partner
Kevane Grant Thornton
E lina.morales@pr.gt.com

Francisco Luis
Tax Partner
Kevane Grant Thornton
E francisco.luis@pr.gt.com

Isabel Hernández
Tax Partner
Kevane Grant Thornton
E isabel.hernandez@pr.gt.com

Kevane Grant Thornton
An instinct for growth™

Kevane Grant Thornton
An instinct for growth™

Advisory

Computer network

Advisory Alert: Think like a cybercriminal to combat threats

The hospital's boardroom is packed. Leadership, department heads, administrative heads and board members are meeting, and a sense of gloom pervades the room. It just may be the end of their world as they know it. A high-profile celebrity patient is dying upstairs. At first it was seen as a medical mistake, but now something more sinister appears to have happened. The news is spreading through social media that the patient is close to death because of a hack into the hospital's systems. Protesters are already gathering out front, asking for a temporary hospital shutdown.

Ojel Rodriguez
Partner Head of Advisory
Kevane Grant Thornton
T (1) 787 754 1915
E ojel.rodriguez@pr.gt.com

Visit our website
www.grantthornton.pr

Introduction

The CEO demands to know how it happened, especially after a recent multimillion dollar investment in improving the hospital's cybersecurity program. The technology team started explaining what they thought happened, describing how they implemented a perimeter security system designed to prevent hackers from gaining access to patient credit card data and health records. In this case, however, the hackers didn't go for any of that — they went straight to the celebrity patient's registration and real-time blood test data and changed his blood group, which resulted in an incorrect blood transfusion. There was a ransom call, but the hospital was too slow to react. The surgery started and the doctors used the wrong blood type, to disastrous effect. The patient is left irreversibly damaged and is expected to die within 24 hours.

The CEO addresses the room with fire in her eyes and says: "How could this have happened? Our business is patient **care** and not patient **data**. We've approached this the wrong way. Fix it!"

Fortunately, this was a cyberwar gaming exercise that Grant Thornton LLP was engaged to perform by one of our hospital clients.

Conventional thinking on cybersecurity is that it is past its expiration date. Companies spend big money to head off cyber-threats, with mixed success. Meanwhile, business leaders routinely acknowledge that attacks against their organization aren't a matter of if, but when. Their nervousness is driven by everyday scenarios of cyberattacks turning into business crises. What's a forward-looking enterprise to do?

The journey from reactive to proactive cybersecurity starts by understanding what is important for the business to grow and thrive.

Reaching a higher state — cybersecurity preparedness 2.0 — forces organizations to acknowledge that they live in an evolving environment. Companies must accept that digital innovation is at the heart of business growth. They must recognize that data is an outcome of that innovation. And they must admit that data can also be a liability. Leaders have to be willing to step into the shoes of cybercriminals, understand the potential motivations and threats these bad actors pose and ultimately come up with proactive strategies to protect their organization's interests.

The journey from reactive to proactive cybersecurity starts by understanding what is important for the business to grow and thrive. The weakest link might be a technology issue plaguing a retail brand. It could be a strategy issue in a life sciences organization. Or it could be a process issue in a financial services enterprise. Regardless of the industry, fostering an understanding of what is truly important for the business is foundational to establishing a sound security strategy.

Treating cyber-risk as separate from other business risks renders it overly technical and mysterious. A more holistic approach to cyber-risk allows companies to place cyber-risks in their proper strategic context and show how management's acceptance of specific cyber-risks will assist — or fail to assist — in creating value. Businesses that fail to enact a strategic approach, and don't include all senior managers in defining and meshing their roles in confronting risk, will continue to be stuck at cybersecurity 1.0.

There are a few obvious hallmarks of companies that are relatively immature on the data-security spectrum:

Letting fear set the agenda

Cyber-breaches can result in costly losses and embarrassing headlines, but fear of breaches can focus management exclusively on point-specific, IT-centric solutions that are regularly leapfrogged by cybercriminals.

Undervaluing digital assets

Companies often assign values to physical assets, but many fail to grasp the true value of all their data, intellectual property and intangible assets such as brand reputation, executive reputation and customer trust. What's more, companies frequently fail to assess the full costs of operational, financial and legal risks that stolen data, compromised transactions and corrupted systems can generate.

Doing an unsatisfactory job defining cyber incidents

These include not only external attacks, but also internal breaches, natural disasters and other events that affect systems and data.

Adopting cyber capabilities without enough strategic contexts

Companies often adopt new technologies — such as mobile devices, social media, cloud computing and artificial intelligence — or form new external partnerships, without considering the full array of risks to their business strategies and changes in their risk appetite that these new ventures may introduce.

The emerging universe of risks will run the gamut — some will be technology issues, but others will be business issues or process issues or people issues. But you'll never know unless everyone is linked to the same effort. Achieving this kind of collaborative approach begins when everyone in a leadership position recognizes the stakes. Getting there requires a few logical steps:

1. **Own the predicament.** Cybersecurity is a top concern of global leaders, as seen in the World Economic Forum's *Global Risks Report 2017*. The issue topped the list of most likely risks in North America. For context, consider that more than five million new devices are activated every day. Analysts predict the number of internet of things devices will soar from more than six billion today, to more than 20 billion by 2020. Connectivity equals risk, and therefore everyone is responsible for cybercrime prevention.[1]

2. **Map business processes, stakeholders and data systems.** Organizations focused on cyber-risk need to adopt the kind of seamless, crash-free and bug-free approach that we see on popular mobile apps — a full-stack view of your assets, consisting of full mapping of business processes, the potential users and related technologies. You need to weigh your cyber-risk by conducting risk assessment of each asset (stack view). Only then is it possible to identify potential risks, consider those risks against risk appetite, and implement controls accordingly. Where risk is elevated, controls need to be higher.

3. **Align, integrate and measure.** It is vital to bring together operational and financial leaders with risk leaders, and align and integrate their goals, objectives, compliance demands, and stakeholder expectations. This will require operational processes to be meshed with cyber controls — with a special focus on where the business is most sensitive. And all this must be overlaid with a system of measurement and metrics, so that leaders always can assess the threat outlook, have options to dial up controls and further enact a digital strategy.

[1] "6.4 billion connected 'things' will be in use in 2016," Gartner, Nov. 10, 2015.

Source: https://www.grantthornton.com/library/whitepapers/advisory/2017/think-cybercriminal-combat-threats.aspx

Conclusion

The key to managing threats isn't necessarily greater investment or even manpower. Instead, it takes the imagination of a criminal — seeing your own enterprise as they would see it. Wherever you are most sensitive is the most likely target of future cyber-threats. What is most valuable to you is also most valuable to someone who wants to hurt you.

Kevane Grant Thornton

An instinct for growth™

Kevane Grant Thornton
An instinct for growth™

Tax

Accuracy

Operational excellence

Outsourcing Alert: Electronic Federal Tax Payment System– New Payment Options

The Electronic Federal Tax Payment System (EFTPS) is a free service from the U.S. Department of the Treasury for organizations, professionals and individuals.

Julio Villegas
Audit Partner and
Head of Outsourcing
Kevane Grant Thornton
T (1) 787 754 1915
E julio.villegas@pr.gt.com

Organizations, professionals and individuals registered with the Electronic Federal Tax Payment System (EFTPS) (meaning having a PIN number) and responsible for making federal tax deposits and or payments are now able to use the EFTPS's website for additional federal tax payments. Other methods as voice response system and special channels continue to be available. The EFTPS's enabled payment options for taxpayers are:

- Federal Tax Deposits
- Balance due on return or notice
- Payment Due on an Amended or Adjusted Return
- Application Fees
- 20% Initial Payment (Cash Offer)
- Accepted Offer
- Subsequent Payment/Installment Agreement
- Audit Adjustment

Please note that tax payments are due regardless of this website's availability.

You can access the voice response system for tax payments at 1.800.555.3453. Follow the prompts to make the payment.

Payments processed using EFTPS website or through the voice response system must be scheduled by **8 p.m. ET the day before the due date** to be received timely by the IRS. The funds will be debited from the bank account on the date you select for settlement.

Call to action
Access our website and visit our Professional articles box
www.grantthornton.pr

Access the following link for more information
https://www.eftps.gov/eftps/

At Kevane Grant Thornton we provide our clients with personalized attention, valuable advice and recommendations, tailored solutions and direct access to technical experts to help clients resolve issues and identify opportunities.

Kevane Grant Thornton
An instinct for growth™