Volume 3: Part 2 2018

The Four T's of local government performance

CGMA

# Technology

## Improving local government performance: strategy, communication and cybersecurity

## Part 2

## Chartered Global Management Accountant (CGMA®)

Two of the world's most prestigious accounting bodies, AICPA and CIMA, have collaborated to establish the Chartered Global Management Accountant (CGMA®) designation to elevate and build recognition of the profession of management accounting. This international designation recognises the most talented and committed management accountants with the discipline and skill to drive strong business performance. CGMA® designation holders are either CPAs with qualifying management accounting experience, or associates or fellow members of the Chartered Institute of Management Accountants.

**cgma.org**

## Association of International Certified Professional Accountants

The Association of International Certified Professional Accountants (the Association) is the most influential body of professional accountants, combining the strengths of the American Institute of CPAs (AICPA) and the Chartered Institute of Management Accountants (CIMA) to power opportunity, trust and prosperity for people, businesses and economies worldwide. It represents 650,000 members and students in public and management accounting and advocates for the public interest and business sustainability on current and emerging issues. With broad reach, rigor and resources, the Association advances the reputation, employability and quality of CPAs, CGMA designation holders and accounting and finance professionals globally.

**aicpaglobal.com**

# Contents

# Introduction

## In this report, we continue our investigation into technological developments in the public sector by considering the role of strategy, communication and cybersecurity in the implementation of technology.

The 2014 CGMA® report, 'Managing local government performance – Transparency, technology, talent and transformation', outlined a new role for finance professionals: helping local authority leaders address key performance management challenges.

The report established that an astounding '89% of respondents identified technology adoption as the biggest area where improvement was needed to benefit citizens, but that only 29% currently used technology to the direct benefit of its citizens'.[1] It concluded that providing transparent, relevant and timely information to support public services and decision making is critical for successful, sustainable government entities.

The research described in the original report explored the local government practices of today and tomorrow in 48 countries. Its findings showed that governments must simultaneously address four key areas and meet the ongoing challenge of 'doing more with less'.

The four key needs are to:

1. actively pursue the **transformation** of public services
2. enable the necessary **technology** to support this objective
3. respond to increasing public demand for government **transparency**
4. contend with the difficulty of recruiting, developing and retaining **talent** in an increasingly competitive market.

Only by addressing these Four T's will governments fulfil the demands of politicians, citizens, businesses and other constituents within increasingly diverse communities.

Our subsequent research considers each of these areas in more detail and provides practical guidance for finance professionals. This briefing, the third in the series, focuses on the development and communication of strategies for digital excellence. It places a particular emphasis on cybersecurity, a topic of continued interest and concern for government organisations around the world.

**Volume 1**: Managing local government performance

**Volume 2**: Transparency

**Volume 3**: Technology

Part 1: digitalisation and open data

Part 2: strategy, communication and cybersecurity

**Volume 4**: Talent

**Volume 5**: Transformation

# Strategies for digital excellence

## Successful digital governments design strategies to promote innovative data-centric services that meet their citizens' needs and demands for services.

Our 2014 survey found that local government finance professionals consider digital technologies to be crucial to current and future success. They also agree that the communication and integration of strategy are integral to that success.

Technological developments in areas like artificial intelligence (AI) and the Cloud are becoming increasingly prevalent within public sector organisations. The role of finance professionals and management accountants is extending beyond awareness of the technology available, what it is and how to use it. To be truly effective, finance also has a major role to play in developing digital strategy, communicating it and implementing the plan.

## i. Development and implementation

**Case study: Seoul e-government**

Today's citizens have high expectations of the digital experience, driven in the main by innovative online retailers such as Amazon and Alibaba. Although government has lagged behind, there is growing recognition that the right digital tools can transform the user experience, improve operational efficiency and ultimately reduce costs. As with any transformation programme, a clearly articulated strategy, understood at all levels, is essential to success.

The performance of Seoul Metropolitan Government, consistently rated as the leading (or one of the top five) e-government in the world, illustrates how effective its long-term strategy has proven to be. Executed in four large steps (Figure 1) over several years, this strategy has resulted in significant achievements.

**Figure 1. Seoul e-government four-step strategy**[2]

The Seoul Metropolitan Government discloses all of its administrative information to citizens and shares public data with them, offering citizens new employment opportunities. It provides citizens with useful everyday information such as bus and subway arrival times, cultural events, job opportunities, and real estate transactions and rentals. The entire range of city administrative services are also accessible via mobile devices and public apps. Citizens can access the information anytime, anywhere.

M-Voting, a mobile voting system, was introduced in February 2014 to improve citizen engagement with policymaking. Citizens can vote on major policy issues using computers or via their mobile phones.

The government's Social Media Center integrates departmental and mayoral social media accounts in order to deliver citizen feedback and requests to the relevant department in a timely manner. To improve transparency, details of all interactions between citizens and public servants are made available to the public.

The Social Media Center acts as a communication window between the city and its citizens, providing vital information such as weather and transportation alerts in emergency situations. It also aims to close the digital divide, supporting the disadvantaged to boost their information literacy.

The Seoul Metropolitan Government continues to expand its services and plan for further growth. In September 2013, it identified 429 distinct types of tasks/information within 327 citizen service areas. It is implementing a four-year plan to expand these to 570 types of tasks/information covering 400 service areas.

One benefit already achieved is the way in which already disclosed public data have motivated the private sector to develop new public services and create jobs. The data have become public properties with new economic values. Seoul National University estimated in 2012 that the disclosure of the city's public data would create an economic value of 2.1 trillion KRW.[3] While this value is of a scale that many smaller local governments may not see, applying the principles involved can and does deliver proportionate economic benefits.

## Social media and risk

Local government organisations globally are increasingly making use of social media to communicate, connect and collaborate with citizens, communities and other stakeholders. Well managed social media usage can foster innovation, knowledge sharing, participatory decision making and the development of citizen-led services that help governments to learn more about the people they serve. But with social media crime on the rise, it is important to be aware of the risks involved.
These include:

- **Loss of control:** accidental or poorly advised postings on social media by an entity or its representatives could go viral, reaching multitudes almost instantaneously.
- **Damaging comments:** negative comments from citizens can seriously damage an entity's reputation.
- **Security breaches:** sensitive or proprietary information could be made public.
- **Hacking:** social media sites are vulnerable to malware attacks and hacking that could result in the loss of an organisation's information and data.
- **Loss of productivity:** employees could spend time using their personal or professional social media accounts for purposes that are not related to work.

Although leaders may have concerns about social media, they generally agree on its growing importance to their organisation.[11]

### Case study - ResilienceDirect

The connective role of technology in bringing together formerly disparate services and departments can drive significant efficiency savings. An example of this is the UK's ResilienceDirect, a multi-agency collaborative network developed and funded by the Cabinet Office.[4] Its business case was founded on delivering savings to the public purse. Designed to cut across multiple communication channels to drive greater efficiency and joint working at strategic and tactical levels, the network has delivered over £760k in efficiency savings.[5]

It helps civil-protection practitioners such as police, fire and ambulance services, local authorities and utility partners to work together across geographical and organisational boundaries during the preparation, response and recovery phases of an event or emergency. Accessible on all mobile devices and using Ordnance Survey mapping data, the platform allows emergency responders to pinpoint risk areas and communicate securely, offering a greater sense of shared situational awareness.

Activities include:

- sharing emergency plans among local, national and sub-national partners
- sharing situation reports and briefings between local responders
- enabling the integrated management of events and consistent provision of information to the public
- communicating situation reports to any lead government departments that are facilitating national co-ordination/action in response to an incident
- managing contact information to ensure a single, up-to-date version of distribution lists
- issuing news and guidance from central government to local responders.

Following the extreme weather of December 2015 in which storms Desmond and Eva flooded over 16,000 houses in England, and the subsequent National Flood Resilience Review, a 'Report a Flooded Property' app was developed. This helps emergency responders by displaying a map of properties reported as flooded, and can identify more widespread flooding problems. Armed with this information, field staff can be sent out as necessary to personally assess the reports and take remedial action. The software can also be used to address problems such as heavy snow, and further developments are planned.

## ii. Communication

Even the best designed strategies fail without stakeholder buy-in. To succeed, digital government requires internal and external take-up. According to OECD recommendations on digital government strategies, governments should not follow their own internal logic and needs when setting up more open approaches to policy-making and public service delivery.[6] Rather, they should re-organise themselves around user expectations, needs and associated requirements. To achieve this successfully requires excellent communication with internal and external stakeholders.

One tried and tested method of communicating strategy is through the use of strategy maps, which describe how organisations create value by building upon strategic themes. They also provide a way to increase stakeholder engagement through telling the story of the strategy. Well-constructed strategy maps describe how the organisation plans to meet specific customer promises through a combination of processes (employee, technology and business) that satisfy customer expectations and meet stakeholder demands. The CGMA Strategy Mapping tool includes a step-by-step approach to developing and cascading strategy maps.[7]

Effective two-way communication is key to ensuring a streamlined and consistent digital experience in the public sector. Connectivity, internet usage, digital public services, integrated technology and assurances of cybersecurity must all be made known to citizens through marketing, instructions and common channels.

The United Kingdom and Northern Ireland takes a whole-of-government approach to online service delivery, to which the promotion and education of staff and users alike is central. Gov.uk, launched in 2012, brought together nearly 1,900 departmental, agency and public-body websites in a single portal. This allows users to view all policies, announcements, publications, statistics and consultations in one place, together with data on service performance and user satisfaction. A UK Digital Strategy was published in 2017, focusing on infrastructure, citizen and business skills, data and cybersecurity.[8]

"For businesses to thrive and grow, government needs to create the conditions and set the framework for investment in widespread and up-to-date infrastructure … Connectivity drives productivity and innovation, and is the physical underpinning of a digital nation."

**UK Digital Strategy, 2017[8]**

Developing a common approach for digital service delivery helps government entities share understanding, knowledge and best practice, and ensure that digital services are fit for purpose. Gov.uk content is required to meet the Digital Service Standard which covers the creation and running of good digital services.[9] Local government followed suit with the launch of the Local Government Digital Service Standard in 2016.[10] This provides local government entities with guidance, suggesting 15 criteria for the creation and running of good digital services. These indicate a clear role for finance professionals, highlighting the importance of project and information evaluation and the building of sustainable multidisciplinary teams to design and lead the service. Solid performance data will also be essential to inform ongoing iterative development.

Translating big data into better decision making and budgetary savings is a skill the local government finance professional of the future is going to need.

### The digital divide

Globally, there is a distinct separation between those people who have access to digital technologies and those who do not. This is the so-called 'digital divide'. For citizens of any government, whether federal or local, there is a risk that those without internet access will be prevented or excluded from using many government services. How do we balance this disparity of provision with the opportunities that online services can create? The solution begins, in many cases, with communication and the creation of a digitally inclusive infrastructure.

Government organisations must encourage people to use digital services, providing assisted digital support if required. The Digital Service Standard includes a direction for government bodies to plan to increase digital take-up (the percentage of people using government services online in relation to other channels, for example paper or telephone). Digital take-up data should be measured every month and shared via a service performance platform alongside key performance indicators for user satisfaction, cost per transaction and completion rates.

Governments seek to improve the lives of the people they serve, and this value can be clearly demonstrated through digital civic engagement. Innovative governments have recognised this opportunity and its related benefits, and are using technology to serve their citizens better. However, there are many challenges for them to overcome. A prime example is how to address users' security concerns.

# Cybersecurity

## The high media profile of cybersecurity issues makes it easy to convince boards of their importance. However, persuading operational staff can be more of a challenge.

An 'it couldn't happen here' attitude can be prevalent. The responsibility for overcoming this often resides with finance professionals. They are seen as stewards and guardians, and their familiarity with risk and control processes means they are well placed to support cybersecurity initiatives.

Organisational culture has been identified as a key cybersecurity risk factor. A sophisticated protection regime that includes website filtering, complex password requirements and two-factor authentication can quickly be made toothless by poor privacy behaviour. Employees can often act on what they see others say and do, and 'rationalised non-compliance' actions such as password circumvention damage security. Research from information services firm CEB has found that in the average company more than a quarter of employees exhibit poor privacy behaviour. CEB suggests four ways to better embed privacy requirements into organisational workflow.

### Four ways to better embed privacy requirements into workflow

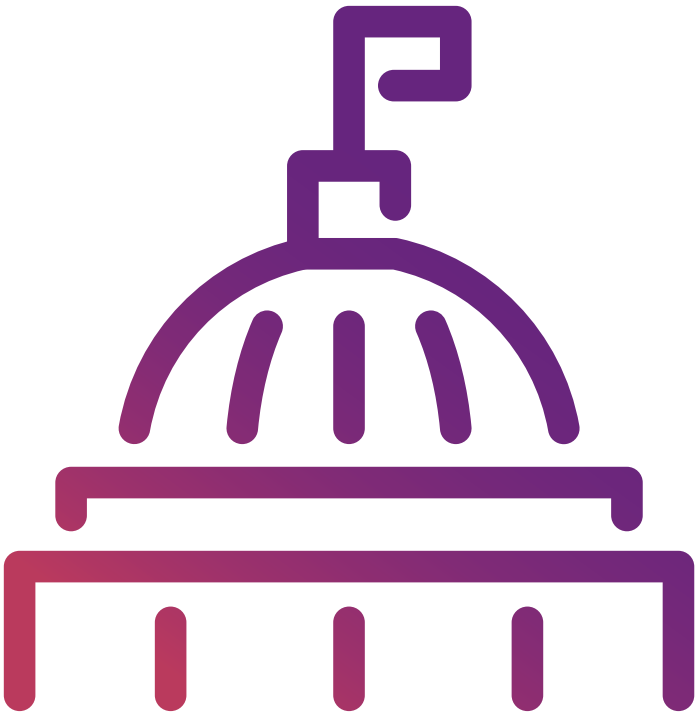
1. **Identify business processes that collect, store and use sensitive data:** not all work involves such data, but areas such as payment transactions or employee/customer health information can be risky.
2. **Identify and address situations where non-compliance is more likely:** one obvious area of concern is devices that aren't company-owned. Without proper precautions, employees who do work on their own smartphones, tablets or laptops can put data at risk.
3. **Rely on managers to drive compliance:** recommend that managers contribute to how privacy requirements align with a team's work. Discuss data security regularly, not as an annual tick-the-box exercise. This way, employees will have a better understanding of its importance.
4. **Use a continuous-improvement approach to aligning privacy requirements and workflow:** leading organisations get real-time feedback about the effectiveness of information controls. That input from workers can help reduce inefficiency and address employee perceptions about policies that might seem unrealistic.[12]

Developing and adopting a risk management framework that addresses an entity's unique situation is the key to the effective navigation and management of cybersecurity. While all government entities share similarities, they are not identical. They have their own unique set of requirements and needs, based on several factors. Having a flexible framework, such as the AICPA Cybersecurity Risk Management Framework, gives a government organisation the groundwork it requires to achieve innovation, ease of implementation and sustainability.

Cybersecurity is, and will continue to be, a very hot topic when technology is discussed, regardless of an entity's size, funding stream or service orientation. Commercial solutions can be expensive, but there are simple and economical steps that management accountants and other finance professionals can take to help protect their organisations against cybercrime.

## The AICPA Cybersecurity Risk Management Reporting Framework

The American Institute of Certified Public Accountants (AICPA) has developed a Cybersecurity Risk Management Reporting Framework to help organisations communicate pertinent information regarding their risk management efforts. This provides a common language and guidance to address the identification, establishment, continued diligence and reporting of a system of controls. The framework calls for management to prepare a narrative description of their risk management programme, together with an assertion of organisational risk control effectiveness.[13]



**1. Know email scams and warn others:**
People are increasingly seeking the weak link in organisations' cyber armour. Everybody knows not to give their bank account details to an unknown dignitary from a foreign government. But what if they get an email from their CEO instructing them to wire funds for a deal that they know is about to close? According to an FBI report, this scenario was all too real in 2016 for a finance employee who was tricked into wiring US$730,000 to a bank in China.[14] Since the FBI started tracking business e-mail scams in late 2013, it has compiled statistics on more than 7,000 US companies that were targeted. Total losses have exceeded $740 million.

**2. Maintain a strong connection with IT:**
Management accountants and IT professionals have a common interest in protecting sensitive and confidential data, and can learn a surprising amount from one another. Management accountants can clearly help IT design cybersecurity controls and develop reports or provide assurance on them. Beyond that, however, there are many low- and no-cost ways they can help IT colleagues to prioritise which information and systems are most sensitive and to balance cybersecurity against operational needs. They should stay connected with IT staff and encourage informal dialogue by holding regular discussions – and even social events – where they can make sure everyone is in accord. Clear priorities help IT work more efficiently and save money in the long run.

**3. Stay on top of free updates and upgrades:**
According to Amy Zegert, Co-Director and Senior Fellow for the Stanford Center for International Security and Cooperation, research shows there is on average one defect, caused by human error, for every 2,500 lines of programming code. Cybercriminals exploit these mistakes to break into systems. Busy users often overlook software updates to correct such vulnerabilities. These are usually free, and should be used on computers, smartphones and any other devices used for business purposes.

**4. Adopt a stronger password policy:**
If a password can be found in a dictionary, it is not secure. Unless special precautions are in place, such as substituting numbers or special characters for letters, it is probably also insecure if the name of a child, pet or spouse is used. Despite the inconvenience, implementing and enforcing a good password policy is a free and simple way to protect data. Good policies should include guidelines on how often to change passwords, where to store them and instructions for creating them.

**5. Develop a plan and practice it:**
This advice appears in every business article about cybersecurity, but its importance cannot be overstated. Management accountants can help by developing and activating the business continuity plan – in this case, the 'cyber incident response plan'.[15] Answers to questions like: 'Who is the cybersecurity representative?' and 'Who outside this office needs to be notified of the breach?' should already exist. Practice exercises will help key people understand their role and enable any issues to be resolved. The plan should be continually updated as new threats arise. When it comes to cybercrime, no one can ever be over-prepared.[16]

The cybersecurity threat landscape can be overwhelming. Many finance executives assume that the responsibility to defend against cybersecurity threats lies in the hands of the IT department or IT consulting group. However, the threats and the fall out associated with a cybersecurity incident can have significant financial impact on an organisation. It therefore becomes the responsibility of the accountant. While finance professionals are not expected to have the IT knowledge required to protect the organisation, from a risk-management perspective it is critical that they should know what to ask and understand the implications of the answers.

Events such as the 'WannaCry' and 'Petya' ransomware attacks exploited vulnerabilities for which Microsoft had previously issued security patches. Yet many organisations were impacted because not all of their systems were up-to-date with the latest patches. Asking the IT department about the systems in place to approve security patches, deploy them and confirm their installation would have saved organisations significant disruption and cost. Assessing vulnerabilities and the associated level of risk is the first step in effectively managing cybersecurity threats.

As well as asking the IT department the right questions, it is important to identify who in the organisation is responsible for ongoing staff-training. While in some cases this is the responsibility of the IT department, in certain organisations another department may be responsible for everything to do with training. That said, training is often an overlooked component of managing cybersecurity risk. Identifying who is responsible for training and connecting them with the IT department to provide the correct tools for ongoing training can make the difference between an employee taking pause for thought and creating a data breach. Cybersecurity threat training needs to be an ongoing initiative that is continuously present for all end-users. The finance executive must work with the correct groups to ensure this is occurring and that information is current, relevant and frequent.

It is critical that the finance professionals and technology managers have a regular and frequent dialogue to discuss security issues and internal initiatives to combat cybersecurity threats. Successful organisations agree and maintain a regular meeting format that includes the discussion and review of topics such as:

- internal events threatening organisational systems and data
- current external cybersecurity threats to be aware of and the measures in place internally to limit risk
- security logs relating to enterprise threat-management systems such as firewalls, intrusion detection and prevention systems and unauthorised authentication events
- ongoing education initiatives for end-users
- new organisational initiatives and potential vulnerabilities that should be considered
- organisational cybersecurity policies to ensure they remain current.

Finance professionals have a key role to play in encouraging management to adopt and communicate robust risk policies, frameworks and processes, all of which help address the inevitable risks of cybersecurity.

Sir Iain Lobban, former director of GCHQ, stated in 2012 that about **80% of known attacks would be defeated by embedding basic information security practices for people, processes and technology.**[17]

Cyber security specialists **Protection Group International** suggest the 'Kiss and Tell' approach to cyber protection:

**K**eep patching up to date

**I**nsist antivirus is active and up to date

**S**ave your files with a good backup regime

**S**ecure your passwords

… and **tell!**

Communication is crucial: staff training and frequent 'cyber conversation' is paramount to the building and maintenance of a strong 'human firewall'. With the majority of data breaches resulting from human error, cybersecurity is as much a 'people problem' as it is a technology issue.

# Conclusion

Regardless of size, status or geography, many of the world's most successful government organisations pay particular attention to the development and communication of strategies for digital excellence.

This helps them to create, deliver and promote data-centric services that meet citizens' needs. Using digital technologies and communications methods is critical to success – and the growing responsibility and influence of finance professionals means they have an increasingly important role to play in both developing and implementing strategy.

Citizen benefit is the most important outcome of a successful digital strategy. To maximise this, government organisations need to encourage greater take-up to eradicate the so-called 'digital divide'.

At the same time, they need to focus more on mitigating any resultant growth in the cybersecurity risks they face, many of which are cultural and individual to the organisation. The AICPA Cybersecurity Risk Management Framework offers the flexibility government organisations need, both to cater for this individuality and to provide the groundwork required to achieve innovation, ease of implementation and sustainability.

Increasingly, management accountants and other finance professionals will partner with IT. This will ensure that government entities have in place the processes and systems needed to manage and safeguard the organisation's integrity, efficiency, security and ability to meet citizen needs.

# Further guidance and resources

The following resources provide definitions, best practices and implementation guidance for government organisations.

A new path for cyber risk management

AICPA Cybersecurity Resource Center: features the latest resources, CPE and guidance on cybersecurity risk management

Cybersecurity risk, response and remediation strategies

Description Criteria for Management's Description of the Entity's Cybersecurity Risk Management Program: intended for use by management in designing and describing their cybersecurity risk management programme, and by management accountants to report on management's description

Technology – Improving government performance: digitalisation and open data

Global Management Accounting Principles®

Integrated reporting in the public sector

The Four T's of local government performance

Transparency – Improving government performance

The hidden costs of a data breach

Learn more about the role finance professionals can play in the cybersecurity landscape and access news and information at the AICPA's Cybersecurity Resource Center. Access targeted resources for finance professionals providing cybersecurity advisory services through the AICPA's Information Management and Technology Assurance Section, including a free podcast on social engineering, a type of cybercrime.

The CGMA local government research programme examines the supporting technology required to enable transformation and sustainability. It considers the effectiveness of responses to public demand for innovative digital solutions in an increasingly competitive market.

Visit www.cgma.org/government to learn more about the programme.

## Cybersecurity risk disclosure

The AICPA Cybersecurity Risk Management Reporting Framework advises organisations to disclose factors with a significant effect on inherent cybersecurity risks. These include the characteristics of technologies, connection types, use of service providers and the delivery channels the entity uses, as well as organisational and user characteristics and environmental, technological, organisational and other changes.

Examples include:

- use of outsourcing such as Cloud computing and IT-hosted services
- use of mobile devices, platforms and deployment approaches
- network architecture and strategy, including the extent of the use of virtualisation
- types of application and infrastructure
- types of service provider that store, process and transmit sensitive data or access the entity's systems
- the size and structure of the IT department
- distribution of responsibilities relating to the cybersecurity risk management programme between business functions
- any changes to the entity's principal products, services or distribution methods
- changes to legal and regulatory requirements.

For additional examples as well as further implementation guidance, please refer to the AICPA's **'Description Criteria for Management's Description of the Entity's Cybersecurity Risk Management Program'** April, 2017©

# Endnotes


1. Managing local government performance, CGMA, 2015, cgma.org/resources/reports/managing-local-government-performance.html
2. Seoul e-Government Report, p. 14-16, 2014, citynet-ap.org/wp-content/uploads/2014/06/Seoul-e-Government-English.pdf
3. Seoul e-Government Report, p. 18, 2014, citynet-ap.org/wp-content/uploads/2014/06/Seoul-e-Government-English.pdf
4. Resilience Direct, Ordnance Survey, 2017, ordnancesurvey.co.uk/business-and-government/public-sector/resilience-direct/index.html#start
5. Resilience Direct, Ordnance Survey, 2017, ordnancesurvey.co.uk/business-and-government/case-studies/resilience-direct.html
6. Recommendation of the Council on Digital Government Strategies, OECD, 2014, oecd.org/gov/digital-government/Recommendation-digital-government-strategies.pdf
7. CGMA tool: How to develop a strategy map, CGMA, 2012, cgma.org/resources/tools/downloadabledocuments/cgma-strategy-mapping-tool-final.pdf
8. Our plan for Britain: Executive summary, Department for Digital, Culture, Media and Sport, 2017, gov.uk/government/publications/uk-digital-strategy/executive-summary
9. Digital Service Standard, Government Digital Service, 2017, gov.uk/service-manual/service-standard
10. Digital Service Standard, Local Government, 2017, localgovdigital.info/assets/documents/local-government-digital-service-standard.pdf
11. James Carberry, Communications – Methods and applications for financial managers, AICPA, 2013-2014, p. 118-119 aicpastore.com/ManagementAccounting/PRDOVR~PC-PCG1301/PC-PCG1301.jsp
12. How a company's culture can limit data breaches, CGMA Magazine, 2016, cgma.org/magazine/2016/nov/how-company-culture-can-limit-data-breaches-201615493.html
13. SOC for Cybersecurity, AICPA, 2017, aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpacybersecurityinitiative.html
14. Business email compromise: an emerging global threat, FBI, 2015, fbi.gov/news/stories/business-e-mail-compromise
15. Are you prepared for a cybersecurity attack?, AICPA, 2015, blog.aicpa.org/2015/09/are-you-prepared-for-a-cybersecurity-attack.html#sthash.88uwF1ZJ.vzhhdFEn.dpbs
16. Susan Pierce, CPA, CITP, CGMA, 5 low or no cost ways for CPAs to help slam the door on cybercriminals, AICPA, 2016, blog.aicpa.org/2016/10/5-low-or-no-cost-ways-for-cpas-to-help-slam-the-door-on-cybercriminals.html
17. 10 Steps to Cyber Security, NCSC, 2012 ncsc.gov.uk/guidance/10-steps-cyber-security

# Authors and acknowledgments


## Rebecca McCaffry, FCMA, CGMA

Associate Technical Director, Management Accounting
The Association of International Certified
Professional Accountants

## Lori A. Sexton, CPA, CGMA

Senior Technical Manager, Management Accounting
The Association of International Certified
Professional Accountants



We would like to thank the AICPA's Government and Performance Accountability CGMA Advisory Group contributors:

Peter Jannis, CPA, ESQ, CFP, CGFO

John Kaschak, CPA, CGMA, CISA, CGAP, CGFM

Carrie Kruse, CPA, CGMA

Jeff Parkison, CPA, CGMA

Ryan Nicholas Paterson, CPA, CGMA, MBA

Richard Scheel, CPA

Susan Simpson, CPA.

These individuals contributed time, knowledge, insight and experience to help shape this report

**With thanks to:**

City of Seoul, South Korea

ResilienceDirect

Protection Group International

aicpa.org
aicpa-cima.com
cgma.org
cimaglobal.com

First published December 2017