1. How Technology is Changing Business Processes in General

Technology is integrated in many of the business processes we work with today. It has automated business functions, including complex and tedious activities, strengthened processing effectiveness and efficiency, and improved, transparency, reporting and oversight. As technology has evolved, data has become more portable and accessible; and systems, devices, and data have become more interconnected.

While technology presents opportunities for improving business processes, there are also many associated challenges and risks (e.g., data security) that need to be properly addressed/managed to protect the organization.

Today, organizations are gravitating to mobile work environments, web-based/online applications and cloud technology. The purpose is to provide access to information to our employees and constituents to help them meet their business needs and continue to provide and receive services efficiently, but at the same time from any available platform. This means access via mobile phones, laptops or workstations. With this availability of tools and information, business processes have changed by eliminating steps and making them more efficient and at times saving on costs as well.

**Mobility/Collaboration**

There are several technologies in place today to encourage and facilitate mobility and provide 24-7, 365-day access. For example, Office 365 tools allows you to provide a mobile work environment, cloud technology or streamline business processes. The mission is to use these ‘out of the box’ tools and make them useful throughout the organization:

- **Outlook Access Online**: Email access available online using your mobile devices.

- **Skype For Business (S4B)** – Provides the ability to conduct remote meeting sessions with employees without need for a physical location or travel time.

- **One Drive for Business (OD4B)** - Provides users additional data, which in turn reduces ISD storage costs, but the real benefit, is offsite access and sharing of your files. You can access your files on your mobile device or mobile workstation.

- **SharePoint Online (SPO)** – Provides out of the box ability to share and seamlessly collaborate. SharePoint workflows are pre-programmed mini-applications that streamline and automate a wide variety of business processes — from collecting signatures, feedback, or approvals for a plan or document, to tracking the current status of a routine procedure. SharePoint workflows are designed to save time and effort, and to bring consistency and efficiency to tasks performed on a regular basis.

- **PowerBI/Tableau** – These two tools are available to employees, allowing end users to create and share information in a visual form to drive change and improve service delivery. With the introduction of Office 365, use of PowerBI is expanding.
Digital Business Transactions

Technology increases automation of the vendor payment process and creates a paperless environment. Technology eliminates the need for physical invoices and payment warrants which mitigates physical theft and loss, mail delays, and printing and postage costs. Technology also enforces processing requirements and controls, and increases accountability by maintaining a digital transaction record. Web-based/online applications are also designed with cloud solutions such as DocuSign and Salesforce allowing for the use of e-signatures, automated workflow and imaging to eliminate paper and manual hand-offs. Below are examples of these types of applications being used throughout California counties:

- **Vendor Direct Deposit Registration Portal** – This allows vendors to submit direct deposit online with the ability to download payment and invoice information. This portal provides the following advantages:
  - Reduces material costs, such as warrants stock, envelopes and postages.
  - Reduces fraudulent activity thereby protecting county assets. Warrants that are stolen can be fraudulently cashed or altered for a higher dollar amount.
  - Less reliance on costly printing and USPS delivery services.

- **Acceptable Use Agreement (AUA) eForms & Digital Signatures** – A mandatory paper form that employees must sign manually can be changed into an automated paperless trackable process with digital signatures.
  An eForm provides the following advantages:
  - Prepopulated eForm data pulled from HR/Financials system, provides error free entry.
  - Reduces paper and printing (toner) costs in submitting a printed paper form.
  - Reduces the process time significantly. The logistics of moving a form to and from employees throughout the organization is eliminated, therefore, reducing the labor costs to complete the process.
  - Monitor AUA process with real-time status to determine location of form.

- **Authorized Approver App** lists users and their backups authorized to sign documents. A simple workflow allows new users to be added easily.

- **CBO Contract Renewals** takes advantage of Salesforce workflow and DocuSign to create and sign contracts for the Social Services Agency, reducing paper by 90%.

- **Workload Distribution Tool** integrated with CalWIN – distributes work to Case managers. The number of apps processed on time increased from 78% to 97%, reducing late penalties.

With regards to citizens, millions of dollars in purchases and payments can be made via mobile and on-line transactions from anywhere at any time:

- Birth/Death/Marriage certificates
- Property Taxes
- Business License Tax
- Central Collections – Debt payments
- Special Events
• Disaster Relief
• ROV E-Store
• Assessment Appeals
• Moving Violations
• Official Public Records
• Permits
• Event fund raising through texting

Citizen Engagement

Expanded use of technology has opened the door to powerful new ways to strengthen ties with the residents and provide them with information about vital county services 24-7, 365 days a year. Civic engagement events like Hackathons bring the community together to educate and help solve local challenges. Broader access to services through technology is also something that tech-savvy constituents have come to expect. Award winning apps and programs have been developed that appeal to all ages using open data, social media, hackathons, mobile/web apps, and websites resulting in innovative government services that allow citizens to share information and communicate with government.

With increased use of smartphones and tablets, the public has quickly come to expect government services to be available anytime and anywhere through their mobile devices. The homeless population now has access to services through smartphones. This growing expectation puts pressure on counties to expand its focus on the use of mobile devices in the delivery of information and services. In a very short period, counties’ focus shifted from creating native mobile apps to developing responsive websites to cater to the needs of mobile device users.

Open Budget websites that include videos, dashboards and interactive data help the community understand and explore our annual budgets.

Unique mobile apps include:

• Emergency Preparedness App – A successful redesign of the site includes rebranding of the site color, layout, and logo; providing concise Emergency preparedness content (text, videos, graphics); providing easy search and navigation; ability to access the site from a desktop, tablet, and smartphone.

• My Poll Worker – Gives each poll worker specific data on their polling location, contact information for their support team, and allows them to view and update their scheduled training.

• Calendar Mobile App – A mobile calendar app that provides up-to-date information about local events. It is a simple calendar/event mobile app for both the public and employees to easily access up-to-date county events such as: public meetings, workshops, trainings, festivals, farmer’s markets, etc.

• Canvassing App – The BizChek Canvassing application enables the Assessor’s Office to utilize mobile devices for their field visits resulting in efficiency and increased revenue.
• **SitStat** – An electronic mapping system (GIS) for county and Municipal Fire and Emergency Medical Services to track emergency incidents and responding units in real-time.

• **Permit Portal**: This is a one-stop multi-modal shop for permits related to Building, Planning, Business License, Well permits, Environment, Food, Restaurant, Tree and Encroachment permits.

• **Map1193 Human Trafficking** - crowdsourcing app to ensure certain establishments are compliant with SB1193. https://www.map1193.org/. Five counties are now using the app with two more on the way.

• **The Open Tree Map** app launched in 2016 created new opportunities for crowdsourced tree inventory, ecosystem services calculations, urban forestry analysis and community engagement.

**Open Data**

Through Open Data, the community is able to access data 24-7, 365 days a year to conduct analysis and even develop their own apps:

• **Alameda County Tax Calculator** – This app uses Alameda County's property tax and assessment datasets to show financial information about a property.

• **AcPaFi (Mobile and Desktop)** – The Alameda County Path Finder app is a versatile 4-in-1 application that serves as a digital pocket guide for citizens in Alameda County. You can use AcPaFi to find new restaurants, schools, libraries, hospitals, etc. in your area.

• **GreenByME** – GreenByME locates certified green businesses in Alameda County – built with the goal of connecting residents and visitors with sustainable green practices of their community.

• **Alameda County Info** – The Alameda County Informational app helps its residents to find information about the county. It includes restaurant inspections, crime statistics, schools, parks, hospitals, health clinics, senior centers, and emergency shelters.

• **Alameda County Access** – Alameda County Access enables residents and visitors to stay up-to-date with county news and events. Citizens can share information with others through social media.

**Social Media**

Social Media is a highly effective approach to inform the public about important issues and engage them in challenges faced by local government. Social Media is how people, especially the younger generations communicate and it can be a key tool in recruiting new talent. The creative uses of Social Media represent just one of many ways technology and innovation are leveraged to keep residents apprised of new processes and products available to them. Social Media platforms used regularly by include Facebook (including Facebook Live), Twitter, YouTube, Vimeo, and Flickr.
2. Use of the Cloud, Data Centers & Data Warehouses

Leveraging cloud-based technologies that are scalable to deliver services in a rapid and cost-effective manner, increases employee productivity while reducing county infrastructure and support costs. Cloud computing is defined as storing and accessing data and programs over the internet. Cloud services can provide economies of scale, allow organizations to reallocate valuable human capital from IT maintenance to business partnerships, and reduce costs. Organizations need to consider the costs, benefits, and risks associated with their data storage and data management options/choices (i.e., Internal vs External/Cloud). This includes understanding the data, its security/protection, and the related costs. Specifically:

- Data – What type of data are we storing (e.g., confidential, or public information)?
- Data Security - How is it protected and what assurance do you have that it’s properly protected? For example, who has access, is the information security infrastructure appropriate, does the personnel have the expertise, etc., and what self-monitoring is done?
- What are the costs of moving to the cloud vs. remaining on-premise?

Often counties function in a hybrid environment consisting of both cloud and On-Premise solutions with a Cloud First strategy. Every new system typically goes through a decision tree:

1) SaaS Provider (Software as a Service)
2) Cloud Service (LaaS - Location as a Service, PaaS – Platform as a Service)
3) Virtualized On-Premise Infrastructure
4) Physical On-Premise Infrastructure

In many counties, work continues to move legacy systems to the cloud, to leverage the most current technology, and provide a scalable and robust infrastructure.

One advantage of using the cloud can be reduced cost. For example, a Public Works department published Road Closures data for Constituents using Amazon Web Services (AWS) and WAZE. The “serverless” solution does not require a large expenditure in “overprovisioning” for continual high traffic volumes. AWS was used to host the application in a Serverless model. The operating costs for the site are < $1 per month. In terms of Resilience and Scaling, it can instantly scale from 1 user to 1 million users at any time, and during an emergency.

Another example is the Alameda County Election Results Viewer (electionmaps.acgov.org) provides a map visualization of election results for local races. The site is mobile friendly delivering timely information. It was scaled up on election day for a total cost of $25.

Alameda continues to leverage its unique partnership with Sonoma County, to provide reciprocal hosting for Disaster Recovery/Business Continuity infrastructure. This partnership provides a cost-effective Disaster Recovery solution, which allows Alameda to utilize already existing resources (real estate, racks, power, etc.) within a fully equipped data center that is further removed from direct effects of a localized natural disaster. The Disaster Recovery site at Sonoma County includes key infrastructure and services, such as: internet
connectivity, core network services, mainframe systems, virtual server environments, storage environments and critical countywide applications.

Examples of cloud-based solutions include:

- Cloud-based applications built through Salesforce, a cloud solution: Constituent Tracking System for Board of Supervisors, Boards and Commissions for Clerk of the Board, CBO Contract Renewals for Social Services, Emergency Tracking for the Sheriff, and Contracts for GSA and ITD. These apps use cloud-based “Serverless” infrastructure that does not require planning of failover or redundancy but has resiliency built-in. “Serverless” architecture provides built-in redundancy for storage and distributed failover of application servers and infrastructure, so that these cloud products can be used without needing a formal Disaster Recovery plan.

- A countywide migration to Microsoft Office 365 greatly strengthens the county’s business continuity posture pertaining to email, file access and collaborative data. This greatly minimizes risk and allows for faster recovery compared to self-hosted exchange environments.

- CYA, an application-aware back-up and recovery software solution that safeguards the IBM FileNet Content Manager platform from data loss and downtime by providing hot, consistent platform backups, ensuring fast recovery from operational incidents and allowing Recovery Point Objectives to be 15 minutes or less in the event of a disaster.

- Electronic Records Retention – makes electronic records available instantly to the public through the county’s website.

- Website transition to SaaS – reduces operating and ongoing expenditures, reduces staff time and increases productivity due to out of the box templates.

- Disaster recovery – migrating server services and disaster recovery data from on-premises, county-maintained hosted model to a cloud-based solution.

- Office 365, Exchange Online and other enterprise applications utilizing SaaS.

3. Cyber Security Issues as Technology Changes

Organizations need an information security program that includes policies and procedures for managing Cyber Security risks and responding to incidents. Security needs to be part of any change in information technology to ensure risks are properly assessed and mitigated before it is implemented/used. Security also needs a strategy for managing and addressing security issues as they occur.

- Are auditing, and reporting processes in place to ensure that data is protected?
- Have the associated costs for the office space, necessary personnel, and IT resources (e.g., Hardware and Software); and or the cost for outsourcing aspects of the function been identified?
With changing and new technology, the dialogue of how does 'Cyber Security' comes into play. The introduction of Office 365, cloud technology and developed online tools/application creates one big question.

With the introduction of these tools and technology, how do you stay secure?

You can’t eliminate all associated risks and vulnerabilities associated with new technology but you can greatly reduce those most likely threats to your data.

Threats come to the county in different ways. Attacks targeted directly at your IT Resources (Online Sites, Servers, Workstations, Mobile Devices).

- **Denial-of-Service (DoS) attack** - where the attackers (hackers) attempt to prevent legitimate users from accessing the service. In a DoS attack, the attacker usually sends excessive messages asking the network or server to authenticate requests that have invalid return addresses.

- **Brute force attack** - is a trial-and-error method used to obtain information such as a user password or personal identification number (PIN). In a brute force attack, automated software is used to generate a large number of consecutive guesses as to the value of the desired data.

Email attacks have become the way bad guys try to take advantage and test your 'security awareness' knowledge.

- **Phishing** - the fraudulent attempt to obtain sensitive information such as usernames, password and credit card details (and money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.

- **Spoofing** - is a fraudulent or malicious practice in which communication is sent from an unknown source disguised as a source known to the receiver.

- **Smishing** - is a type of phishing attack where mobile phone users receive text messages containing a web site hyperlink, which, if clicked would download a Trojan horse to the mobile phone.

- **Malware** - malicious software that can easily be described as unwanted software that is installed in your system without your consent. Viruses, worms, and Trojan horses are examples of malicious software that are often grouped together and referred to as malware.

- **Ransomware** - malware may change the victim’s login credentials for a computing device; in a data kidnapping attack, the malware may encrypt files on the infected device, as well as other connected network devices. To decrypt, the victim will need to pay a ransom.

The key to addressing the above 'attacks' is to empower all of the county’s staff to be ready to ward off any such attacks on a one-on-one basis. The introduction of new technology and tools give you more than a ‘fighting chance’ if you mobilize all of your employees.
Furthermore, as technology changes so must the strategy on how you implement Cyber Security and address threats to the countywide network. You can’t be caught standing still in this regard. The hackers are never idle in inventing new ways to attack your data. Your strategy starts with the Chief Information Officer and Departmental Executive Members’ Information Security staff. They need to develop a comprehensive strategy supported by relevant policies and resources backed-stopped with on-going training that ensures all the county staff are effective team members.

A good link for more information on the above topics is:


**Products to Consider**

Office 365 Microsoft provides a secure environment and is compliant with relevant privacy and security regulations. Microsoft provides statuses of continuous audited controls from global information security standards and regulations. Office 365 has conducted the following:

- **Audited Controls**
  - **ISO 27001-2013**: Office 365 has been accredited to latest ISO 27001:2013 standards. Information under this standard will help you to understand how Office 365 has implemented Information Security Management System (ISMS) to manage and control information security risks. In addition, you will gain deep insights into implementation and testing of controls to maintain Confidentiality, Integrity, and availability of your data.
  
  - **ISO 27018-2014**: In line with Office 365's commitment to maintain strict privacy of your data, Office 365 has been accredited to latest ISO 27018:2014 standards. In this section you will see implementation and testing of controls specific to protection of Personally Identifiable Information (PII) and Privacy
  
  - **NIST 800-53A (Rev. 4)**: Office 365 has been accredited to latest NIST 800-53A (Rev. 4) standards. Information under this standard can help you better understand how Microsoft has implemented an Information Security Management System to manage and control information security risks related to Office 365. In addition, this information provides you with insights into the implementation and testing of controls designed to maintain the confidentiality, integrity, and availability of customer data in Office 365.

**Information Security Program**

However, strengthening your Cyber Security efforts starts with the implementation of an Information Security Program that integrates IT security into its IT environment and county culture (remember every employee is a resource to you in thwarting hackers.)

Some counties have established and or adopted the following in thwarting the hackers:

- **Information Security Committee** – Promote IT security, develop policies/standards and implement IT security tools.
- Countywide IT Security Policies – Revised
- County Security Standards & Directives – Mobile Access to Office 365 Resources
- Tools implemented – CISCO Umbrella, CISCO AMP

- **Cybersecurity Workgroups** – Workgroups that develop baseline standards/guidelines in the security areas below and address these risks and vulnerabilities.
  
  - **Applications Cybersecurity Workgroup** – Provides guidance on how to develop more secure applications.
  
  - **Endpoint Cybersecurity Workgroup** – What do we implement physically and logically to secure our endpoints? *(Endpoint security)* refers to a methodology of protecting the corporate network when accessed via remote devices such as laptops or other wireless and mobile devices. Each device with a remote connection to the network creates a potential entry point for security threats.
  
  - **Incident Response Cybersecurity Workgroup** – Develop methods and procedures to ensure quick and responsive measures are taken to stop and react to cyber incidents including pre-authorized contractors to assist the county in every phase of investigation and response.
  
  - **Computer Incident Response Teams (CIRT)** – Respond to cyber incidents aggressively and efficiently.
  
  - **Network Cybersecurity Workgroup** – Implement measures to ensure your networks are secure from attacks.
  
  - **Risk Management Cybersecurity Workgroup** – Provide assessment and guidance on how to remove, avoid or mitigate risks.
  
  - **Policies Cybersecurity Workgroup** – Provide countywide guidance, standards and policies on what to protect and how.
  
  - **Education and Awareness Cybersecurity Workgroup** – Provide county employees the tools and knowledge to avoid becoming a victim of attacks or cyber fraud.

- **Security briefings to Executive Management**

- **Annual Mandatory Countywide Security Awareness Training**

- **Development of Departmental Information Security Program SharePoint Site** to provide the Department with a one-stop shop for all things IT security related.
  
  - Information on the Departmental Information Security Program (DISP)
  
  - DISP Projects and Activities
  
  - Information and easy access on how to report incidents
- Tips on how to stay secure
- News and events – provide upcoming calendar events such as October’s National Cyber Security Awareness Month

4. Conclusion

Technology has already significantly changed how we do business at a revolutionary pace and it has just begun! Technology is like the tide, it’s coming whether you are ready for it or not, so embrace technology in the work-place as readily as you did the 60-inch Flat Screen TV.

- The most successful response to the technological changes, opportunities and threats that are already lapping at your feet (whether you noticed or not) is to be pro-actively engaged with the possibilities, good and bad.

- Learn from others ‘mistakes’ and challenges and assemble a team of knowledgeable business and IT expertise, be their in-house of outside consultants, and work to assess your most likely vulnerabilities and their corresponding solutions.

- Address the easy and most often exploited weaknesses first and do so continually and aggressively.

- Empower each one of your employees to be the First Line of Defense against hackers and abusers of technology and to be the champions of change through continuous training, mentoring and engagement.