Insights on governance, risk and compliance

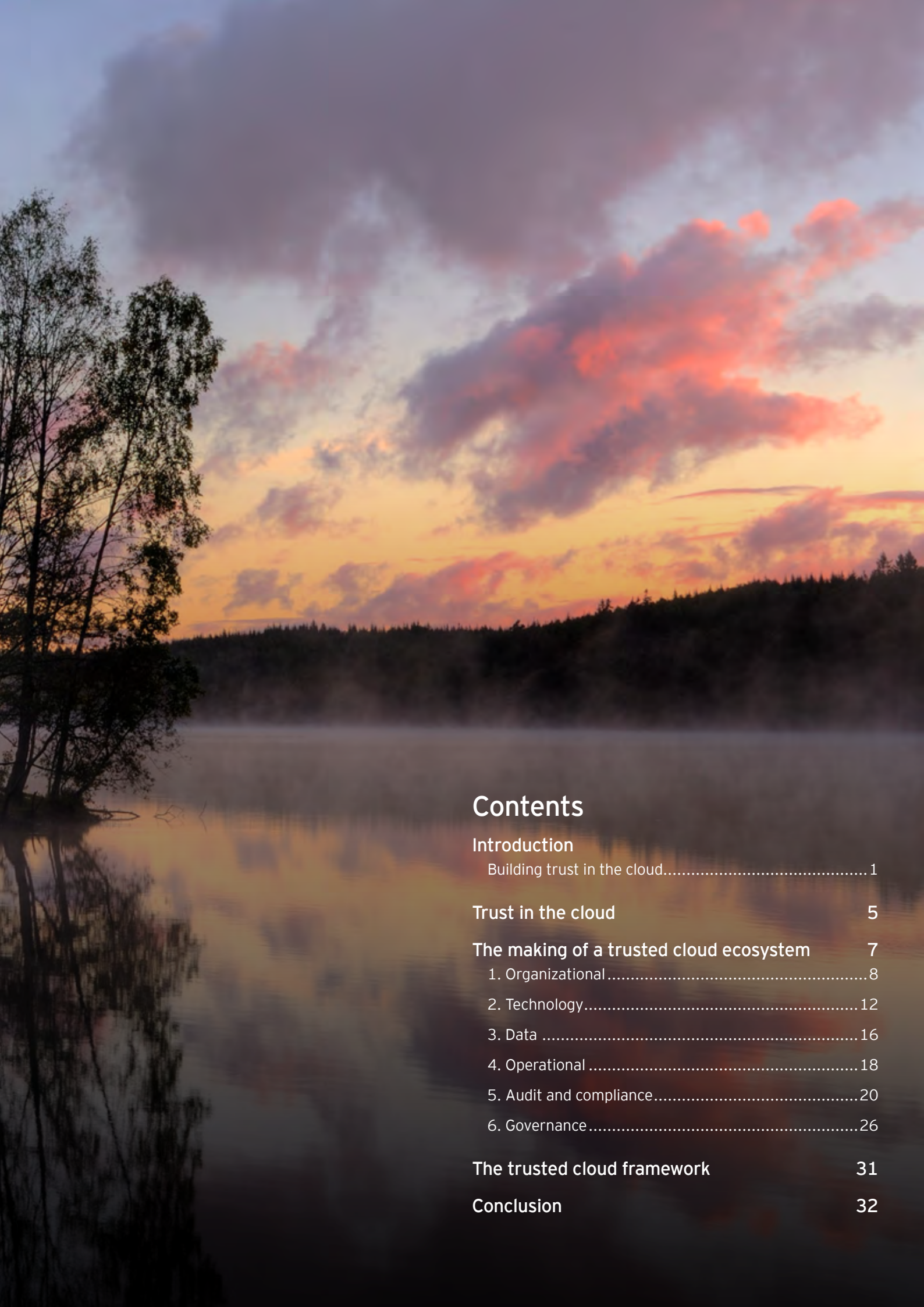
June 2014

Building trust in the cloud

Creating confidence in your cloud ecosystem

EY

Building a better working world



Contents

Building trust in the cloud

Fifteen minutes and a credit card. That is all it takes for anyone within an organization today to set up a cloud solution. This ease of access is one of many reasons individuals, business units and departments are using cloud service providers with increasing frequency.

In late 2013, International Data Corporation (IDC) released a forecast anticipating that worldwide spending on public IT cloud services would reach $47.4 billion. By 2017, its forecast suggested this number would exceed $107 billion.[1]

Yet, despite the rapid escalation of cloud services use, many IT executives remain hesitant to endorse a "cloud-first" approach. Worse, there are some who refuse to adopt any cloud-based services at all, citing security and privacy concerns, operational challenges or inability to control information once it leaves the perimeter. According to a Forrester Research survey, 50% of businesses in Europe and North America identify security as the number one reason for not having adopted cloud computing.[2] Respondents to *Under cyber attack: EY's Global Information Security Survey 2013* mirrored this concern, with 25% reporting that cloud computing use had most changed their risk exposure in the last 12 months.[3]

Unfortunately, this attitude can increase an organization's risk rather than mitigating it. In order to meet fierce competitive demands and new business requirements, many organizations have found internal stakeholders will procure cloud computing services directly, without involving IT experts and thus leaving the associated risks unmanaged.

So what should IT executives do?

1 *IDC*, "IDC Forecasts Worldwide Public IT Cloud Services Spending to Reach Nearly $108 Billion by 2017 as Focus Shifts from Savings to Innovation," 3 September 2013, accessed 18 April 2014. http://www.idc.com/getdoc.jsp?containerId=prUS24298013.

2 Ed Ferrara and Andras Cser, "Security's Cloud Revolution Is Upon Us," Forrester Research, Inc., 2 August 2013.

3 EY, *Under cyber attack: EY's Global Information Security Survey 2013*, 2013, http://www.ey.com/Publication/vwLUAssets/EY_-_2013_Global_Information_Security_Survey/$FILE/EY-GISS-Under-cyber-attack.pdf.

IT executives need to consider the full range of risks involved in their on-premise and externally hosted cloud environments that comprise their ecosystem.

The best option is to develop a holistic cloud trust strategy — one involving key stakeholders from both the business and IT to provide a secure cloud ecosystem with the proper checks and balances that enable a controlled and cost-effective investment in the cloud.

By developing a cloud trust model to assess and monitor, improve and enhance, and certify and comply their cloud ecosystem, IT professionals can turn fear of the cloud into an opportunity to address increasingly complex security and privacy challenges.

IT executives need to consider the full range of risks involved in their on-premise and externally hosted cloud environments that comprise their ecosystem. The goal is to maintain a similar risk exposure or even achieve a lower risk exposure, particularly as information and functionality are moved from in-house to external providers. Due to volume and scale, cloud service providers (CSPs) may be able to invest more in physically securing facilities where information is stored or in network devices with more advanced capabilities. On the other hand, a less vigilant CSP may try to hold down overhead costs by refusing to invest in these additional — and sometimes necessary — security controls. It is also important to keep in mind that cloud service consumers (CSCs) will continue to own certain controls even as they invest in cloud services.

Creating a model that maps who owns what controls is one of the first steps in looking beyond a secure stand-alone environment and moving to a trusted cloud ecosystem.

Cloud services options defined

CSPs offer a wide spectrum of services. They generally fall into three categories:

1. **Infrastructure as a service (IaaS):** IaaS capabilities include processing, storage, networks and other fundamental computing resources where the consumer is able to deploy and run software, including operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage and deployed applications and perhaps limited control of select networking components (e.g., host firewalls).
2. **Platform as a service (PaaS):** PaaS enables the consumer to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the CSP. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems or storage, but has control over the deployed applications and possibly application hosting environment configurations.
3. **Software as a service (SaaS):** SaaS enables the consumer to use the CSP's applications running on a cloud infrastructure. The applications are accessible from various client devices through a client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

By developing a cloud trust model to assess and monitor, improve and enhance, and certify and comply their cloud ecosystem, IT professionals can turn fear of the cloud into an opportunity to address increasingly complex security and privacy challenges.

Trust in the cloud

Between 2010 and 2012, cloud adoption rates nearly doubled. Yet some IT executives remain skeptical that the benefits of endorsing a cloud-first approach outweigh the risks.

Some fear that communicating information over a public network will increase its technology surface area and make them more vulnerable to cyber attacks. Others worry that CSPs offering the same infrastructure to multiple clients in multiple locations will be unable to maintain segregated confidentiality. Still others express concern that transmitting their information across international boundaries will expose them to diverse legal and regulatory requirements in jurisdictions with which they are unfamiliar.

These concerns are understandable, particularly given one of the traditional principles that has served as the foundation of information security: take control of your environment. It may feel counterintuitive for an organization to surrender control of its IT infrastructure and information to a third party; however, it may be one of the most effective ways to rapidly secure the ecosystem.

Unfortunately, resisting or flat-out rejecting cloud solutions often leads to "cloud creep," shadow IT solutions, increased risk exposure or an overall lack of control in the organization's extended computing environment.

Instead of saying "no you cannot," IT executives need to learn how to confidently say "yes we can." They need to shift their focus toward building a trusted cloud ecosystem.

Instead of saying "no you cannot," IT executives need to learn how to confidently say "yes we can." They need to shift their focus toward building a trusted cloud ecosystem.

Trusted design

A cloud ecosystem with trusted design has the right controls in place to safeguard and protect the underlying computing and information assets. The controls are designed to address the key areas of risk and are strong enough to match the threats to the environment. Both the CSP and CSC are responsible for designing effective cloud controls to manage risk in their respective environments.

Trusted execution

A cloud ecosystem with trusted execution has the right controls in place and is operating effectively per the trusted cloud design. The controls are working as intended and are strengthened when risk indicators rise. The CSP generally has responsibility for control execution while the CSC is accountable for governing and verifying the control objectives are met.

Trusted certification

A cloud ecosystem with trusted certification has been independently tested and verified that the controls are in place, functioning as designed, operating effectively and have been attested to by a certifying body. The CSP has responsibility for attaining the trusted certification status while the CSC reviews and understands the scope and relevance of the certification on the consumed service.

Trusted cloud ecosystem

Your cloud ecosystem should be:

Secure

A secure cloud ecosystem has the appropriate controls to protect the confidentiality, availability and integrity of the systems and data that resides in the cloud. Appropriate procedural and technical protections are in place to protect data at rest, in transit and in use.

Trusted

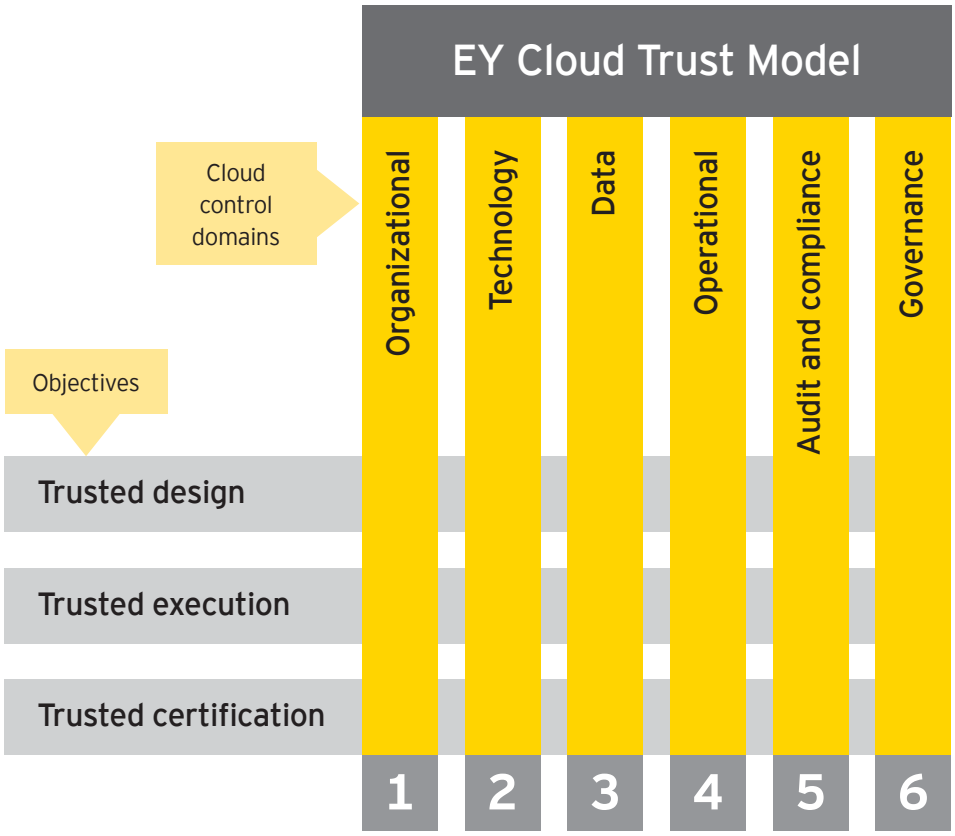
A trusted cloud ecosystem is designed to stand the test of time. It should provide high availability and resilience to adverse events.

Audit-ready

An audit-ready cloud ecosystem has continuous compliance and is certified to meet specific industry regulations and legislation. Appropriate procedural and technical protections are in place and documented and can be verified for compliance purposes.

The making of a trusted cloud ecosystem

Six key dimensions serve as the blueprint for IT executives on their journey to build a trusted cloud ecosystem. These dimensions, which align to the Cloud Security Alliance's Cloud Control Matrix, form a model that helps organizations understand the characteristics of a trusted cloud ecosystem and provides the guidelines to deliver on them.



Building trust in the cloud requires you to look beyond your own cloud environment and establish controls for the entire ecosystem of connected environments.

1. Organizational

Organizations place their information at risk if they do not have proper hiring protocols in place that consider the type and sensitivity of information the employee will have access to — regardless of whether it is stored in the cloud.

An organization's risk exposure is affected, in large part, by the users of its cloud ecosystem. Both internal users and CSP staff who have access to the cloud ecosystem can introduce risk.

To manage these risks, many organizations choose to update roles and responsibilities. Moving to a cloud-based model represents a shift away from "operators" of the technology environment to "governors" of the ecosystem, a new IT operating model that presents different challenges and issues. Some organizations have gone so far as to create new positions and organizational roles to deal with these emerging cloud challenges.

Organizations need a trusted cloud approach where employees and executives feel comfortable about the people with elevated privileges in the cloud.

Inadequate human resources processes

Organizations place their information at risk if they do not have proper hiring protocols in place that consider the type and sensitivity of information the employee will have access to — regardless of whether it is stored in the cloud. High-value intellectual property or highly regulated information may require personnel to commit to appropriate employment agreements before starting with the organization. It is also important to assign, document and communicate roles and responsibilities for employment. If the CSP is managing the information, these requirements may need to extend to its staff with access to the cloud ecosystem.

Because cloud resources are easily accessible, without suitable procedures in place, organizations could experience inappropriate access and loss of confidential information. Human resources departments need to work closely with IT to ensure termination policies and procedures are strictly followed and executed. Training programs should enforce key expected behaviors to make sure employees and control owners understand how their actions work to achieve a trusted ecosystem. Training compliance should be tracked and monitored to ensure accountability and acknowledgement of these responsibilities.

External party risk

External parties with access to the organization's cloud ecosystem pose a security risk. Organizations should subject all employment candidates, contractors and third parties to the necessary screenings proportional to the information classification level to be accessed, the business requirements and acceptable risk. They should also ensure the right contractual protections are in place.

Misuse

Employees may be unfamiliar with how to use cloud resources, and this poor understanding may weaken security controls or risk information loss. Organizations should document roles and responsibilities associated with the use of cloud services and train employees regularly on these protocols.

BYOD and mobile device policies

The use of personal devices spreads information and applications over a wider footprint. Organizations adopting cloud services must consider whether to allow access or connections from these devices. Controls protecting the device or securing information in transit may not be available in all cases. It is important for the organization to understand the information being stored in the cloud and how it can be accessed through mobile paths (by their staff) and then manage the associated risks appropriately.

Managing access over time

A common challenge for organizations is maintaining the "principle of least privilege." This challenge is further complicated when organizations adopt cloud services. Organizations should limit access and permissions to organizational assets to only those with legitimate business need. Organizations should share access requirements with the CSP. At the same time, the CSP must manage access of its staff with access to cloud services.

Questions for executives

- Do we have the appropriate cloud policies and procedures in place to manage personnel with access to cloud resources? Do they have the right competencies and training?
- What are we trying to accomplish with the cloud? Which areas within our organization would benefit the most from cloud solutions?
- How sensitive is our business and employee information? Is our organization subject to industry-specific information security and privacy issues beyond those enforced by US and foreign data privacy laws?
- How is the organization structured? Is a cloud vendor easily able to support a more complex business model?
- Do I have staff available to manage and monitor one or more SaaS, IaaS or PaaS vendor agreements?

1. Organizational

A common challenge for organizations is maintaining the "principle of least privilege." This challenge is further complicated when organizations adopt cloud services.

Actions to consider

Cloud service consumers (CSCs)

- Work with legal counsel and human resources to understand the hiring and screening requirements based on the information handled and geographic location
- Implement documented and understood employee termination and asset return policies and procedures to minimize likelihood of unauthorized access from a terminated employee
- Document roles and responsibilities of contractors, employees and third-party users as they relate to information assets and security
- Develop a BYOD strategy and approach to determine if and how information stored with CSPs can be accessed with personal and/or mobile devices
- Make employees aware of their roles and responsibilities for compliance with established policies and procedures and with maintaining a safe and secure working environment

Cloud service providers (CSPs)

- Provide means or processes to manage and secure mobile devices which have access to CSCs information, with controls that include: the ability to remote wipe information on the devices if it is lost; password and PIN requirements to access the device; encryption and backup of information stored on the devices; control of the applications which can be installed on the device; and anti-malware or malicious application technology on the device itself
- Manage roles/responsibilities and access for each employee with access to cloud services and customer information
- Upon termination of a customer contract, return all of the customers' assets within an established time period
- Identify, document and regularly review requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of information and operational details
- Develop a BYOD strategy and approach to determine if and how cloud services can be accessed or maintained from personal devices
- Implement flexible security measures that allow CSCs to adhere to their regulatory compliance practices
- Implement a security awareness and training program for all contractors, third-party users and employees, with periodic updates to address new threats

US automotive company uses cloud playbook to reduce risk and empower the business

The situation: A US automotive manufacturing company was fielding a barrage of requests for cloud services from the business. The company did not have a cloud strategy and found that many of those requesting the services did not fully understand the implications and risks associated with hosting a solution in the cloud. Without a clear understanding of the risk impact to the business and without a defined cloud strategy, some business owners were bypassing IT to directly purchase cloud services.

The solution: EY worked with the company to develop a cloud computing playbook to educate the organization and lay the foundation for evaluating whether a cloud solution was the right approach for a particular business need. The playbook explored the key considerations for cloud deployments around governance, security, privacy, availability and numerous other domains. The team also made certain that the playbook was easy to read and understand by people outside of IT. The goal was to empower business owners to make informed decisions based on risk and to encourage them to approach IT for further guidance.

The benefit: The playbook enabled the business to ask the right questions of CSPs to make certain that the company's information and assets were protected in the cloud. It also gave the business a clear understanding of cloud services and their inherent risks. Perhaps most importantly, the playbook helped the business see IT as a partner.

The goal was to empower business owners to make informed decisions and to encourage them to approach IT for further guidance.

2. Technology

Without proper identity and access management (IAM) controls, or the application of segregation of duties, neither the organization nor the CSP will know who has access to which data or application.

The underlying technical configuration of the controls that exist in the cloud can make the difference between a trusted ecosystem and an inevitable breach.

Encryption and key management

Clearly, encryption is an important control as an organization's data travels back and forth over the internet and when it is hosted in the CSP's environment. Some CSPs may not have a well-integrated encryption system, nor do they provide total control of the keys to the end user. Organizations should be comfortable with the type and strength of the encryption mechanisms used as well as how encryption keys are managed. Controls should be at least as secure as what is used in on-premise solutions, if not greater.

Identity and access management

Without proper IAM controls, or the application of segregation of duties, neither the organization nor the CSP will know who has access to which data or application. When considering cloud services, organizations will want to work closely with the CSP to establish processes and technical controls for managing access and enforcing stringent access rights as users change over time. If high-value assets, such as intellectual property, are stored with the CSP, organizations should consider additional controls, such as multifactor authentication, beyond a standard username and password. At the same time, the CSP will want to limit access to sensitive customer information by its staff.

Infrastructure and virtualization security

The nature of cloud services relies heavily on network infrastructure and virtualization technologies. Through virtualization, a CSP can provide almost limitless individual (virtual) machines to a CSC very quickly. Yet, with virtualization come a number of risks, including cyber attacks, inter-virtual machine attacks, communication blind spots, operating system hardening, network and hypervisor security.

CSPs need to provide proper assurances that the technology components responsible for creating and running the virtual machines is adequately secured. In terms of infrastructure, the CSP must have strong network management controls, including network architecture that balances and controls traffic appropriately, patching of servers, and the ability to monitor traffic and proactively identify events.

Threat and vulnerability management

As new threats and vulnerabilities emerge, companies need defined processes for anti-virus, patch and vulnerability management. Vulnerability and patch management should follow a standard process and monitor for new threats as they emerge. Organizations should monitor new and emerging vulnerabilities and patches on all end user devices. It is also important that both the organization and the CSPs have defined, documented and tested policies and procedures for threat response in the cloud environment.

Application programming interface (API) security

APIs are used when devices or other services communicate with the cloud service itself. These interfaces can be quite powerful as they allow for manipulation of data sets to support business processes. However, while allowing information to be exchanged between two parties, they are vulnerable to attackers seeking to compromise a service or information. CSPs should offer standard APIs that can be regularly tested and kept up to date.

Questions for executives

- Does the CSP have the right technical controls in place to handle our data?
- What is the best practice for encrypting cloud data? Is our information encrypted in the cloud or in transit to the cloud? Who controls the keys and recovery process?
- Is our CSP virtualization environment hardened or configurations tested?
- How do I control mobile devices, and how secure is the company's environment?
- How do I manage our users' accounts and their access centrally? How do I define and enforce IAM policies in the cloud ecosystem?
- How does the CSP manage threats and vulnerabilities in the cloud ecosystem?
- Are the APIs used to manipulate our cloud data secure?

2. Technology

As new threats and vulnerabilities emerge, companies need defined processes for anti-virus, patch and vulnerability management.

Actions to consider

CSCs

- Monitor vendor cloud security environment to make certain that it matches or exceeds the organization's policies and procedures
- Establish IAM processes to manage users centrally, control segregation of duties and maintain principle of least privilege of access
- Ensure that the CSP agrees to enforce threat and vulnerability management activities in the cloud ecosystem
- Consider evaluating the CSP on infrastructure management and related controls, scalability and flexibility, access to skilled talent, encryption and key management processes, available APIs, and whether key control remains with the organization or the CSP

CSPs

- Work with customers to maintain access requirements in a timely fashion
- Manage staff access to cloud services and customer data
- Maintain industry certifications and offer audit reports to CSCs to prove compliance with stated technical controls
- Offer robust and widely accepted encryption mechanisms to secure CSC data including good key management practices
- Implement standard APIs for ease of data manipulation while completing regular testing and keeping them up to date
- Harden virtualization technologies by locking down configurations and monitoring new vulnerabilities

Leading financial institution conducts a cloud database review to manage inappropriate access and reduce risk

The situation: A leading financial institution was grappling with internal and external compliance issues and requirements. External regulators and internal audits had identified several issues with employee and privileged access to significant financial applications, ranging from a lack of controls on high-risk databases to terminated users retaining access to data.

The solution: EY used its IAM methodology and a cloud-based access and recertification application to address compliance issues. In particular, the EY team leveraged a cloud-based access and recertification application that helped the client create custom workflows for different database types, regions, level of employees and data type, as well as reporting and entitlement revocation workflows. EY also assisted in the deployment of the application in a SaaS model, providing the client with a cloud-based managed service that enabled rapid customization and managed fluctuations in demands.

The benefit: By using the cloud-based access review application, the company was able to improve workflows and its ability to respond more effectively to compliance issues and requirements. The company was also able to reduce the risk of inappropriate access that had been causing frustration and compliance issues.

EY used its IAM methodology and a cloud-based access and recertification application to address compliance issues.

3. Data

The use of cloud services often results in the organization's information assets being physically stored in new geographic locations, including new countries.

Maintaining information assets is a challenge for many organizations. To adequately protect information assets, organizations first need to understand what information assets they possess and how valuable they are. This understanding becomes more important as information moves to the cloud, where more users can access it, including CSP staff, third parties and employees.

Information storage and use

The use of cloud services often results in the organization's information assets being physically stored in new geographic locations, including new countries. As legal and regulatory obligations vary from country to country or even from state to state, organizations and CSPs need to work together to build a complete understanding of where the information will be located, how it logically and physically moves throughout the CSP's environment and what protections are applied to information assets.

Organizations should also understand requirements and activities from regulatory bodies regarding access to encrypted information. Governments or other regulatory bodies may require access to this information in the interest of national security. It is important for organizations to understand these requirements and work with the appropriate legal teams to understand the potential impacts to the organization.

Information ownership and classification

Without an inventory of information assets, organizations cannot know what data they have or how valuable it is. Information classification and handling requirements help communicate the value of information assets, maintain an inventory of the assets and develop processes to properly protect it.

To support proper handling of information assets, the organization should adopt an information classification schema with handling guidelines for each classification. This gives information users the ability to quickly identify the value of the asset to the organization, along with instructions for protection. The handling guidelines provide a set of requirements to be met or exceeded by the CSP in storing the data.

Confidentiality and data protection

Moving data to the cloud does not preclude or eliminate the requirements for confidentiality and data protection. At times, moving data to the cloud can increase the complexity of protecting data as well as the risk of exposure. Information traversing public networks is more vulnerable to attacks from external parties. As a result, organizations and CSPs need to pay particular attention to how these transactions are protected during storage, processing and transmission.

Actions to consider

CSCs

- Evaluate the sensitivity of the information assets you will be storing with the CSP, and provide information classification and handling requirements for information transmittal and storage
- Understand the differential controls applied to more sensitive data
- Verify that the CSP uses security monitoring and logging processes to prevent information loss and exposure
- Assign an owner for each information asset who is accountable for understanding how the asset interacts with and is protected by the CSP; share this information with the CSP
- Understand the physical location where the data will be stored and the applicable laws and regulations of local jurisdictions

CSPs

- Understand the CSC's information and protection requirements for its transmission and storage, and identify a point of contact for each information asset to support the implementation of protection requirements
- Establish policies and procedures, with supporting business processes and technical measures to inventory, document and maintain flows for information with the applications, infrastructure network and systems components
- Investigate the requirements of regulatory bodies, particularly those relating to privacy and credit card data or regulated data such as Protected Health Information; work with CSCs to understand the obligations for each party and how the cloud service provider will fulfill its obligations
- Establish policies and procedures for labeling, handling and securing of CSC information assets and CSP systems impacting the consumer's assets
- Implement security mechanisms to protect information at rest and in transit, such as SSL for secure transit, encryption for data at rest and monitoring for anomalous traffic, which could be an indication of an attack

Questions for executives

- What are the legal, regulatory and contractual obligations impacting the company's information assets? Has our organization adopted information classification policies and procedures with associated handling requirements?
- Has information classification and ownership been shared with the CSP?
- How is information protected when it is transmitted between the on-premise environment and the cloud?
- How is the CSP protecting the company's information as it is transmitted and stored?
- How does our vendor detect a compromise or intrusion?
- How do we control and access our data after it is moved to the cloud?

4. Operational

As the CSC gives up control of IT operations to the CSP, the same due diligence over IT activities needs to be completed as if the function was operated in house, with the CSC and CSP working together to achieve a clear and shared understanding.

Moving from an on-premise solution to a cloud solution has a significant impact on IT operations. Organizations can vastly improve their efficiency, provided they take steps to establish governance, address controls related to foundational security, manage physical and environmental risks, and plan for continuity and recovery scenarios.

IT operations management

As the CSC gives up control of IT operations to the CSP, the same due diligence over IT activities needs to be completed as if the function was operated in house, with the CSC and CSP working together to achieve a clear and shared understanding.

Prior to selecting a CSP that will assume some functions of the in-house IT operations department, organizations should verify a CSP's ability to align its IT operations processes to well-known industry standards as part of its selection criteria. Frameworks such as the Control Objectives for Information and Related Technology (COBIT) or the Information Technology Infrastructure Library (ITIL) provide a basis of industry-accepted processes to create IT policies, standards and procedures. The CSP should also have a program in place to monitor compliance to these governance commitments.

In addition to verifying the operational controls, organizations and CSPs should negotiate a quality control process, including testing and acceptance criteria for each service to ensure the CSCs business needs and service-level agreements are met.

Physical and environment risks

When it comes to physical and environmental risks, the size and scale of a CSP may enable greater investment in controls than is possible for a single organization in an on-premise scenario.

The CSP should be able to provide assurances it is prepared for disruptions in power and utilities and potential natural disasters, with backup arrangements in place to maintain service continuity.

In addition, organizations will want assurances from CSPs in terms of physical access control, limiting access to only those with a business need. Consideration should also be given how information assets are physically moved, replaced or disposed of to ensure suitable protection.

Business continuity and disaster recovery management

When it comes to business continuity and disaster recovery, organizations will want to work closely with the CSP to ensure proper planning and risk mitigation. CSPs will need to have plans for outages and other events. At the same time, organizations will want to create their own plans to manage CSP service disruption. Both the organization and the CSP should also monitor geopolitical factors, such as the potential for civil unrest and the risk it presents.

These plans should include activities such as backing up information assets and other resources, identifying dependencies between systems, determining and prioritizing the criticality of assets and systems, defining lines of communication during an event, documenting roles and responsibilities in a recovery scenario, and maintaining recovery procedures.

Questions for executives

- With what industry standards does the CSP align itself to manage the IT operational environment?
- Does the CSP effectively manage IT operational activity and the related information security risks?
- Is our CSP's data center physically secure?
- How well do our business continuity management and disaster recovery plans integrate with the CSP?

4. Operational

In addition to verifying the operational controls, organizations and CSPs should negotiate a quality control process, including testing and acceptance criteria for each service to ensure the CSCs business needs and service-level agreements are met.

Actions to consider

CSCs

- Select CSPs that align to, use and leverage well-known and accepted industry standards
- Evaluate CSP management of IT operational activities and the impact on related security risks
- Establish criteria for acceptable service levels
- Work with the CSP to implement and test business continuity and disaster recovery plans

CSPs

- Align with industry standards such as COBIT and ITIL
- Create policies, procedures and controls to effectively manage the operations of the service ecosystem and build consumer trust in cloud
- Build physically robust and secure facilities, with supporting processes and procedures
- Establish communication mechanisms with consumers to communicate risks or issues of the service, especially during service disruptions
- Work with CSCs to integrate into their business continuity plans

Global technology company averts disaster with continuity management plan

The situation: A large global technology company needed to develop business continuity management processes so that it could offer new service availability as well as data backup and recovery in a cloud ecosystem.

The solution: EY assisted the organization with developing methods and tools for a business continuity management framework. The team also recommended a road map for rolling out the framework enterprise-wide, helped to complete business-area road maps, identified key performance indicators and coordinated an integration framework with the client business process team to aid in migration efforts.

The benefit: The organization was able to implement an ongoing management and governance process to identify the impact of potential losses, maintain viable recovery strategies and plans, and promote continuity of products and services in the cloud environment.

EY assisted the organization with developing methods and tools for a business continuity management framework.

5. Audit and compliance

Compliance with policies, procedures and the regulatory requirements to which an organization is subject is essential to demonstrate to auditors and assessors.

Organizations need to support audit and compliance functions by implementing robust verification and compliance procedures. A practical approach to audit and compliance in the cloud should include a coordinated combination of consistent and defined internal policy compliance, regulatory compliance and independent auditing. Compliance activities should be defined and agreed upon by applicable groups to confirm support.

Audit and compliance functions assessing cloud technologies should perform initial data gathering to understand where the cloud is deployed, the cloud service model(s) used and the information or transactions processed in the cloud. Once data is identified, the audit function should establish audit plans and activities, including regularly scheduled independent reviews and assessments. These reviews will address any issues in established policies, procedures or contractual and regulatory compliance. An inventory of the organization's legal, statutory and regulatory compliance should be documented and updated regularly.

Contractual obligations

The CSP's standard terms of service may not address an organization's compliance needs. As such, organizations should have legal personnel involved early to validate that cloud services contract provisions are adequate for compliance and audit obligations.

Organizations should make certain that they have a right-to-audit contract clause whenever possible, particularly when using the CSP for a service for which the customer has regulatory compliance responsibilities. Over time, the need for this right could be reduced and in many cases replaced by appropriate third-party assurance reports or certifications.

Audit requirements

Compliance with policies, procedures and the regulatory requirements to which an organization is subject is essential to demonstrate to auditors and assessors. Few IT regulations were established with cloud computing in mind. Auditors and assessors may not be familiar with cloud computing generally or with a given cloud service in particular. Thus, it falls upon the organization and CSP to provide:

- Defined, documented and regularly updated inventory of applicable regulations that affect the use of a given cloud service
- Clear definition of compliance responsibilities between CSP and the organization
- CSP's ability to produce evidence needed for compliance
- The organization's role in bridging the gap between CSP and auditor/assessor

CSP compliance requirements

At a minimum, CSPs should have a third-party assurance report (such as SOC1, SOC2 or SOC3 depending on the needs) as it will provide a recognizable point of reference for auditors and assessors. CSPs seeking to specifically certify their information security environment can adopt the ISO/IEC 27001 standard. ISO/IEC 27001 certification is available to organizations that request third-party certification assurance and are then able to provide this certification to its customers.

Questions for executives

- What third-party assurances does our CSP offer?
- Are there any regulatory requirements of our business that can complicate our use of the cloud?
- How do our cloud-based solutions provide a real-time view of compliance across the organization?
- How are employees keeping up with compliance requirements as cloud adoption increases across the organization?
- Are independent reviews, audits and other assessments conducted at least annually?
- Are all legal, regulatory and compliance obligations and requirements identified and updated based on the assets, type of date and geolocation?
- Are audit plans, activities and operational action items designed to minimize the risk of business process disruption?

5. Audit and compliance

At a minimum, CSPs should have a third-party assurance report (such as SOC1, SOC2 or SOC3 depending on the needs) as it will provide a recognizable point of reference for auditors and assessors.

Actions to consider

CSCs

- Determine audit requirements for CSPs and their ability to perform third-party audits
- Understand and be able to relay the compliance requirements to your CSP
- Select a CSP with a history of transparency in security and policies built into the cloud platform
- Clearly define the roles and responsibilities between the CSC and the CSP
- Gain an understanding of the certifications and compliance that can be leveraged from the CSP

CSPs

- Provide regulatory inventory based on the location of the cloud information being stored and regulations applicable to CSCs
- Provide built-in capabilities and controls to help CSCs meet both industry regulations and internal compliance requirements
- Conduct independently verified, third-party audits to validate that the cloud offering meets industry standards and certifications
- Provide a comprehensive data processing agreement to address both the privacy and security of customer data, helping cloud consumers to comply with local regulations

Global technology company seeks third-party certification for cloud services

The situation: A large global technology company wanted to receive third-party certification, including ISO 27001, to give clients confidence in its services and expand its client base, preferably prior to any going into production.

The solution: EY provided an ISO 27001 certification across multiple cloud-based products. Additionally, the team assisted with scope changes every following year to add more applications to the certification scope.

The benefit: The technology company gained efficiencies through control testing across multiple audits and certifications, including SOC1, Federal Information Security Management Act (FISMA) and ISO 27001. The certification also enabled the company to expand its business into areas where certifications are mandatory business requirements. The company was also able to provide existing clients the confidence they needed to continue using their services.

EY provided an ISO 27001 certification across multiple cloud-based products.

6. Governance

Many organizations believe that the responsibility for accountability, oversight and transparency transfers to the CSP when the data does, which is generally not the case.

Accountability, oversight and transparency are paramount in the cloud ecosystem. Well-developed governance results in scalable programs that are repeatable, measureable, defensible and constantly improving.

Risk management

Many organizations believe that the responsibility for accountability, oversight and transparency transfers to the CSP when the data does, which is generally not the case. Organizations can implement policies, standards and procedures as part of the Information Security Management Program (ISMP) to establish baseline security and risk management process requirements. Organizations should integrate these requirements and hold their CSPs to them. At the same time, CSPs need to understand the requirements of their customers and integrate them into their own ISMP.

Incident management

The unfortunate reality of today's business environment is that incidents are inevitable. Organizations and CSPs need to work together when creating incident response plans to confirm organizations are prepared and appropriately addressing incidents.

Incident response plans should define lines of communication, provide for evidence collection and include procedures and protocols for notifying the CSP or the organization and third parties. Part of an incident response plan should include internal and external points of contact. These plans should be updated regularly as preparedness will help to limit the impact of an incident.

Supply chain and vendor risk management

Organizations should review risk management and governance of supply chain partners and vendors. Each supplier should provide evidence of its information security programs through third-party audits, assessments or other internal assessments. Supply chain checks should also include data quality error checks. Controls should be designed and implemented to ensure adequate security and privacy measures are implemented to all links in the cloud supply chain.

Electronic discovery and cloud forensics

Electronic discovery and forensic processes should be implemented in the cloud and available to CSCs and CSPs when needed. In certain litigations and investigations, the actual cloud application or environment could itself be relevant to resolving the dispute in the litigation or investigation.

Actions to consider

CSCs

- Educate users on the cloud and how to adhere to company governance of the cloud
- Determine a mechanism to regularly evaluate the effectiveness of security measures, including but not limited to incident response process and plans
- Determine security metrics and whether the CSP is delivering against the metrics
- Understand communication process if a security incident affecting your information is identified at the CSP
- Review contract obligation and requirements during instances of electronic discovery and litigation process
- Implement a risk management program and framework that takes into account CSP risks and risk treatment plans

CSPs

- Establish periodic meetings with consumers to communicate risks or issues of the service
- Conduct periodic risk assessments considering compliance with regulatory requirements, policies and contractual terms
- Make electronic incident reporting available for affected customers
- Review risk management practices of CSCs and partners to verify that practices are consistent and aligned to account for risks inherited from other members of that CSP's cloud supply chain
- Maintain and update applicable points of contact for regulation authorities, national and local law enforcement, and other legal jurisdictional authorities
- Implement proper forensic procedures, including chain of custody, to enable the preservation and presentation of evidence to support potential legal action subject to any incident

Questions for executives

- Is a governance model in place to manage the transition and operation of the information flow from our organization to the cloud?
- Has our organization performed a formal risk and security analysis on the information that is being transitioned to the cloud?
- Is the cloud integration strategy in line with management's risk appetite?
- How does the risk of deploying or maintaining an on-premise solution compare with leveraging a cloud service?
- Which independent assurance reports or certifications regarding information security and data protection does our CSP offer?
- How can we ensure the quality and security of our data?

6. Governance

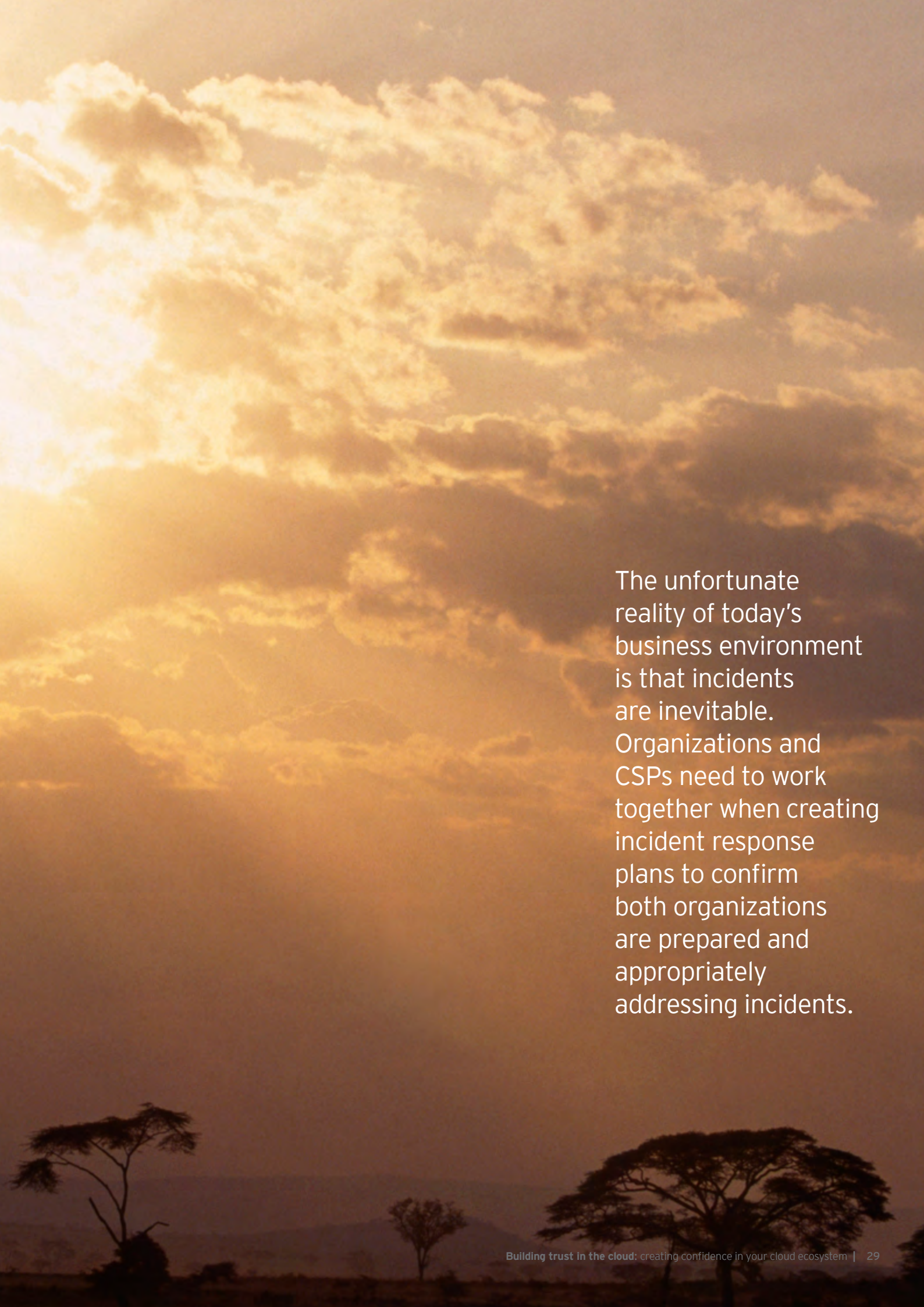
EY helped the client to establish a cloud governance committee and an integrated enterprise resource allocation committee.

National retailer develops cloud governance structure for better organizational alignment

The situation: A national retailer wanted to establish governance processes and structures that enabled the company to develop a cloud strategy that aligned with the business, identified the right initiatives, allocated the appropriate technology resources and managed risk and compliance.

The solution: EY helped the client to establish a cloud governance committee and an integrated enterprise resource allocation committee. The team also developed a governance committee toolkit that helped the organization implement and run the new operating model.

The benefit: The organization was able to refresh and formalize its cloud strategy that aligned to the business, provide direction to achieve the strategy and monitor performance against the strategy.



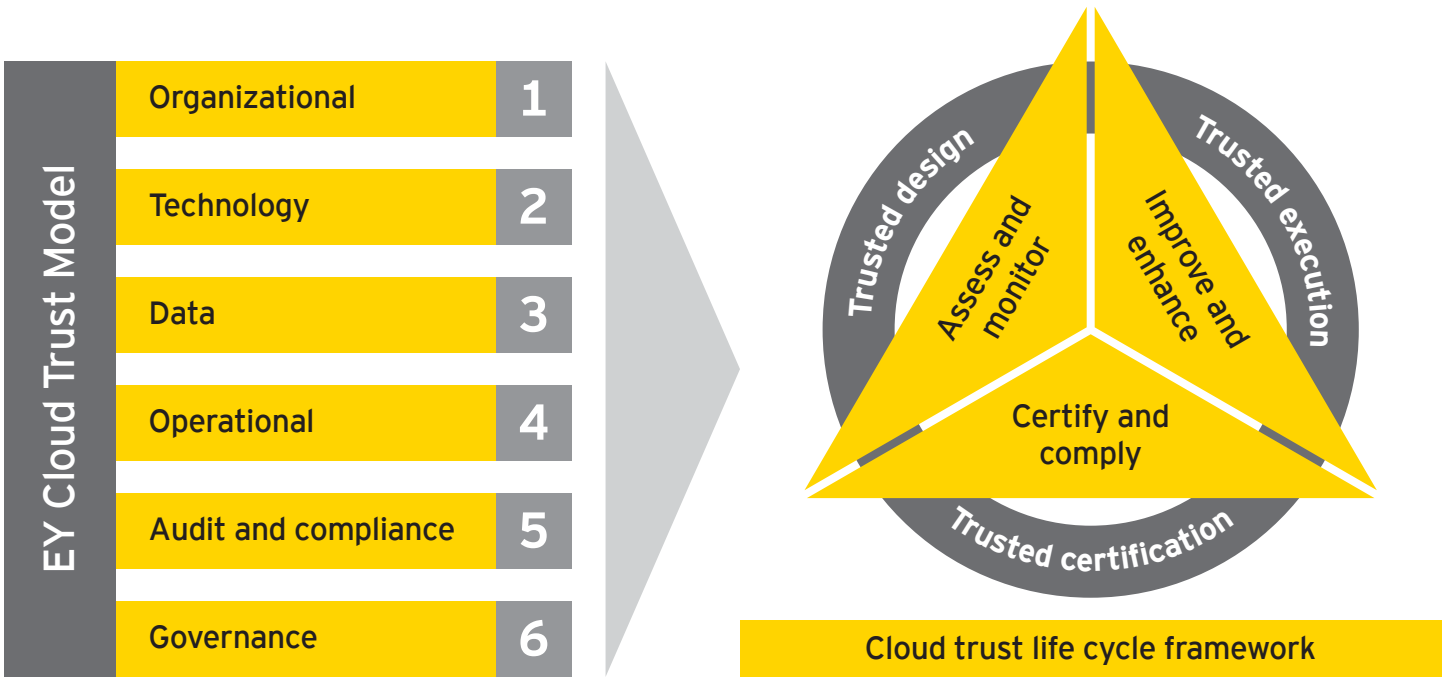
The unfortunate reality of today's business environment is that incidents are inevitable. Organizations and CSPs need to work together when creating incident response plans to confirm both organizations are prepared and appropriately addressing incidents.

The trusted cloud framework

Using the EY Cloud Trust Model as a foundation, organizations can create a cloud trust life cycle framework through which they can build and implement a trusted cloud ecosystem.

This framework will:

- **Assess and monitor** by evaluating the organization's current risk profile and then developing a plan to address key areas of exposure
- **Improve and enhance** by executing remediation activities that support the plan
- **Certify and comply** by obtaining third-party assurance that the organization's cloud ecosystem is secure, trusted and audit-ready



Cloud computing has reached a tipping point

The key is to balance the risks with the value the cloud service provides to the business.

Cloud computing has reached a tipping point as many organizations have either adopted or are planning to adopt some form of cloud computing technology — whether IT knows and manages it or not.

By leveraging the EY Cloud Trust model based on six cloud control domains, organizations can build and implement a trusted cloud ecosystem. The key is to balance the risks with the value the cloud service provides to the business. In many cases, CSPs can offer improved controls to mitigate risk than an on-premise solution. It is up to IT executives to evaluate risk holistically and work with their peers to understand the pros and cons of an on-premise solution versus a cloud solution.

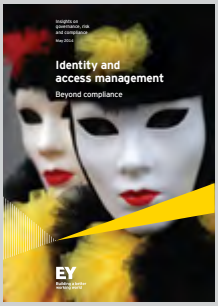
Those in charge of IT departments should view cloud services as another tool in their toolbox. CSPs can take advantage of their scale and specialization to offer IT services at a lower cost to the organization than standing up and maintaining an on-premise solution. Those organizations that remain skeptical of cloud computing and its competitive advantages risk falling behind their competitors. Those that have embraced a cloud-first approach that manages risks through the EY Cloud Trust model are benefiting from the efficiencies, cost savings and additional capabilities that cloud brings. It is time for every organization to embrace a cloud-first perspective or endure the strategic and financial risks that accompany a do-nothing approach.

Want to learn more?

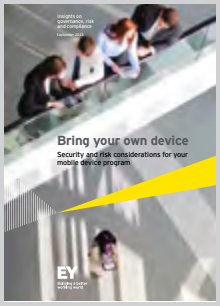
Insights on governance, risk and compliance is an ongoing series of thought leadership reports focused on IT and other business risks and the many related challenges and opportunities. These timely and topical publications are designed to help you understand the issues and provide you with valuable insights about our perspective.

Please visit our *Insights on governance, risk and compliance* series at ey.com/GRCinsights.

Under cyber attack: EY's Global Information Security Survey 2013
ey.com/giss2013

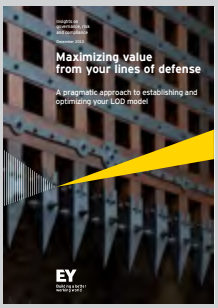


Identity and access management: beyond compliance
ey.com/IAM



Bring your own device: security and risk considerations for your mobile device program
ey.com/BYOD

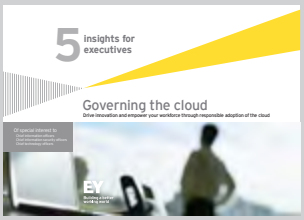
Security Operations Centers against cybercrime: top 10 considerations for success
ey.com/SOC



Maximizing value from your lines of defense: a pragmatic approach to establishing and optimizing your LOD model
ey.com/LOD

Privacy trends 2014: privacy protection in the age of technology
ey.com/privacy2014

Centralized operations: the future of operating models for Risk, Control and Compliance functions
ey.com/centralops



Governing the cloud: drive innovation and empower your workforce through responsible adoption of the cloud
ey.com/GL/en/Services/Advisory/governing-the-cloud

Building trust in the cloud: creating an environment that is secure, trusted and audit-ready
ey.com/GL/en/Services/Advisory/Building-trust-in-the-cloud

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

EYG no: AU2494
1405-1256298 EC
ED 0115

In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

ey.com/advisory

About EY's Advisory Services

Improving business performance while managing risk is an increasingly complex business challenge. Whether your focus is on broad business transformation or more specifically on achieving growth and optimizing or protecting your business, having the right advisors on your side can make all the difference.

Our 30,000 advisory professionals form one of the broadest global advisory networks of any professional organization, delivering seasoned multidisciplinary teams that work with our clients to deliver a powerful and exceptional client service. We use proven, integrated methodologies to help you solve your most challenging business problems, deliver a strong performance in complex market conditions and build sustainable stakeholder confidence for the longer term. We understand that you need services that are adapted to your industry issues, so we bring our broad sector experience and deep subject matter knowledge to bear in a proactive and objective way. Above all, we are committed to measuring the gains and identifying where your strategy and change initiatives are delivering the value your business needs.

To find out more about how our Advisory services could help your organization, speak to your local EY professional or a member of our global team, or view ey.com/advisory.

The leaders of our Risk practice are:

Global Risk Leader		
Paul van Kessel	+31 88 40 71271	paul.van.kessel@nl.ey.com
Area Risk Leaders		
Americas		
Jay Layman	+1 312 879 5071	jay.layman@ey.com
EMEIA		
Jonathan Blackmore	+44 20 7951 1616	jblackmore@uk.ey.com
Asia-Pacific		
Iain Burnet	+61 8 9429 2486	iain.burnet@au.ey.com
Japan		
Yoshihiro Azuma	+81 3 3503 1100	azuma-yshhr@shinnihon.or.jp