EY CertifyPoint benchmark report

Strengths and challenges from 2018 to 2019 around maintaining and operating an information security management system

September 2020

EY
Building a better working world

Contents page

Authors

Jatin Sehgal
Partner
EY Consulting Netherlands LLP

Pratham Jalan
Manager
EY Consulting Netherlands LLP

Tim Preston
Advisor
EY Consulting Netherlands LLP

About this report

This report aims to provide insights on the trends that EY CertifyPoint has seen during ISO/IEC 27001:2013, ISO/IEC 27017:2015 and ISO/IEC 27018:2014 audits it has performed from 2018 to 2019. These insights were identified by collating data across 200+ audits from 65+ clients (from various industries and of different sizes) on the key findings and strengths that were raised during the certification audits, as well as data on the certification scopes and how they changed over the years. This data was then analyzed to identify correlation and trends to provide an overview of industry trends and typical challenges and pitfalls with managing an ISO certification program in the company.

The report also aims to provide the reader with leading practices to follow when undertaking such a program and the benefits of using the information security management system (ISMS) to better manage information security and cybersecurity in the organization.

1 What is EY CertifyPoint?

EY CertifyPoint
Contact:
Antonio Vivaldistraat 150
1083 HP Amsterdam
The Netherlands

Email:
certifypoint@nl.ey.com

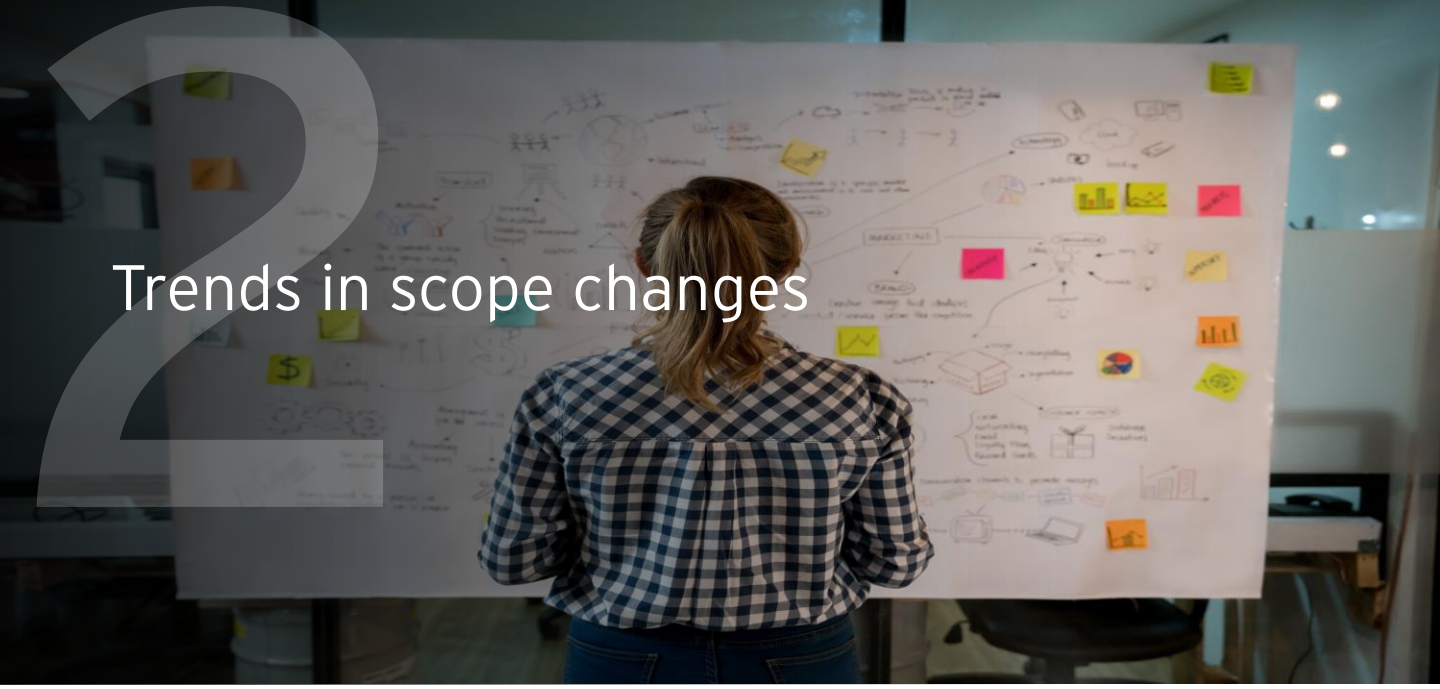
Website:
ey.com/certifypoint

Founded in 2002, EY CertifyPoint is an accredited, independent and impartial certification institute with experienced auditors all over the world, certifying some of the top international organizations.

EY CertifyPoint is responsible for decisions about the granting, maintaining, extending, restricting, postponing and withdrawing of certifications for various ISO standards and other certification frameworks. We perform the complete certification path in accordance with procedures and guidelines, which are included in specific quality manuals per "type" of certification.

Moreover, as we collaborate with experienced professionals within the EY organization, we can provide clients with knowledgeable, experienced and highly qualified auditors who focus not just on compliance, but also on effectiveness. We want to help clients maximize the benefits of certification.

Certification is more than just being compliant to a standard – it's about continually improving the business to achieve operational excellence. EY CertifyPoint supports clients in meeting their goals by improving the efficiency and effectiveness of their management systems. We keep the business at the center, identifying areas of redundancy, bottlenecks and potential efficiency gains by means of a systematic and independent certification approach against a globally recognized standard.



2 Trends in scope changes

Trends of certification scope changes

From 2018 to 2019, 48% of organizations increased the number of locations within the scope of their ISMS. In addition, 67% of organizations increased the number of full-time employees within the scope of their ISMS.

Location increase

36%

Average percentage of increase of locations in scope of ISMS certifications from 2018 to 2019

Headcount increase

23%

Average percentage of increase in employees in scope of ISMS certifications from 2018 to 2019

The reason that the change in locations is greater than the change in employees is most likely due to the higher frequency at which data center or colocation office locations are onboarded or added to the existing management systems, given that these locations frequently have no (or very few) full-time employees in the scope of the ISMS.

This significant increase in scope may be due to the fact that either:

1. Organizations are growing rapidly in size, and as a result the scope of the management system is also expanding rapidly with the organization.
2. Organizations have started with a smaller scope during initial certification process and are now expanding their scope rapidly to the broader parts that were not included in scope to create more trust in the marketplace.

It was unclear from the data which of the two is the likely reason for the significant increase in the scope of the certification for the ISMS for organizations.

Although the scopes of the management systems have significantly increased in the previous years, there have been challenges with onboarding new locations (see "What is not going well" herein for further details and leading practices associated with onboarding new areas to the existing management systems).

As organizations grow in size and complexity, managing the scope of the information security systems becomes more challenging to integrate existing processes and systems into the new areas. These areas could be new products, services, locations, people, departments, functions, innovations, tools, or even entities or companies.

3 What is going well?

1. Top management's involvement and commitment to improve information security and cybersecurity

Across organizations, top management has consistently shown involvement and commitment to the management of information security and cybersecurity, for example by aligning information security and cybersecurity activities to business objectives or by embedding information security processes within organizational processes (ISO/IEC 27001:2013, Clause 5.1, *Leadership and commitment*). This is consistently true across large, medium and small organizations.

Findings

3%

Findings and improvement areas issued against leadership and top management topics in 2018 and 2019

Commitment from leadership and top management is critical to the success of any information security and cybersecurity project in an organization.

The role of the Chief information security officer (CISO) has become more critical than ever before to effectively liaise between the board and the IT functions in an ever-increasing and rapidly changing threat landscape.

Leadership and commitment of the top management starts right from the onset of any information security program that an organization undertakes, e.g., an ISO 27001 certification program. It should be the responsibility of top management to communicate the expectations clearly from the program and set clear outcomes and objectives. Further, top management should be involved in the program throughout its life cycle. This can be done by continuously monitoring the objectives at regular intervals and modifying or setting new objectives once the initial outcomes are reached. Further, providing adequate resources (people, processes, budget and technology) to achieve the desired results, and setting up open communication channels to get outputs from the program and provide inputs to steer the program in the right direction is also a key activity.

Leading practices for information security leadership:

- Sufficiently allocate resources (people, processes and technology) and budget to teams managing and operating the certification program (or any other program)
- Create open communication channels for information security topics to provide inputs to steer the program in the right direction and to get outputs from the program
- Communicate the importance of effective information security and cybersecurity in the organization to all end users and the effects on the organization in case of a breach
- Promote a culture of continual improvement pertaining to information security management throughout the organization and not shying away from findings and deviations identified in the audit process
- Set clear outcomes and objectives of the program, monitoring these objectives at regular intervals and modifying or setting new objectives as the results are realized
- Ensure the safety of all personnel and strengthen and communicate the remote working policy of the organization in the time of a global pandemic
- Undertake various training and awareness not only for end users but also for the board and C-suite-level executives to cascade the importance of the program, the return on investment and the need for information security in the organization

2. Information security in supplier relationships

The management of information security in supplier relationships was a consistent strength across organizations. For example, information security requirements for suppliers are defined, documented and addressed within the relevant supplier agreements. (ISO/IEC 27001:2013 Annex A.15 contains controls related to the management of information security in supplier relationships.)

Please note that the scope of this report does not include privacy as a topic. Privacy is only considered to a small extent when addressing the processing of personal information in public cloud (ISO/IEC 27018:2019). When defining information security, we consider only confidentiality, integrity and availability of information as per the ISO/IEC 27001:2013 standard. Privacy as a criteria is included in the ISO/IEC 27701:2019.

Companies continue to increase their third-party ecosystem for many essential business reasons such as revenue growth, operating efficiency and cost management. As companies enter into these relationships, the data and technologies being used by and with third parties may introduce security risks.

Findings

6%

Findings and improvement areas issued against information security management in supplier relationships in 2018 and 2019

It has become more important to be transparent in the market with the usage of third parties and the shared responsibilities of customers, third parties and organizations.

Some of the key risks from a cybersecurity and information security risks have been managed well. These key risks include:

- Management of cloud applications and products: Along with the increase in the use of third parties, the number of third-party applications are also on the rise. As enterprises shift to cloud-based platforms, each application may pose a unique risk to network and data security.
- Increased volume: While companies may outsource or co-source non-core business-processing responsibilities to third parties, they remain accountable for any adverse events involving their third parties.
- Reputational risk: Publicly disclosed security incidents may adversely impact the brand and even stock price of the affected company.
- Legacy third-party systems: Presence of legacy systems and software at the third party may lead to more vulnerabilities that expose the organization's data to considerable security risk.

Leading practices for managing information security in supplier relationships:

- As companies continue to expand their third-party ecosystem, the security of the third parties involved in their value chain must be evaluated in order to confirm that they do not pose a security risk. Organizations should ask themselves the following questions to understand their security risk exposure and subsequently protect that which is of the most value to their organization and their reputation:
  1. What services do my third parties provide?
  2. What type of data can our third parties access?
  3. Which third parties have access to critical data?
  4. Which third parties have access to our network?
  5. How do third parties access our data?
  6. Do we have the correct mitigating controls in place?
  7. Do the third parties have mitigating controls in place?

The key components when managing third-party risks include:

1. Governance and oversight: Establish guiding principles, organizational structure, policies and procedures, and operational expectations for running the program. This involves:
   - Establish the program strategy and design
   - Assign roles and responsibilities for the team
   - Define awareness and training needs
   - Establish inventory of third-party contacts and their suppliers (if any)
   - Define the risk acceptance, transfer and mitigation thresholds
   - Document the policies, standards, processes and controls

2. Sourcing and due diligence: Create business case for contracting, adopt a risk intelligence approach to understand cybersecurity risk posture, and establish security expectations. This involves:
   - Assess cybersecurity risk posture using external intelligence (e.g., ISO certification, SOC 2)
   - Establish third-party cybersecurity risk profiles
   - Document a cybersecurity risk model
   - Tier third parties based on risk classification criteria

3. Contracting: Begin negotiations with third party and establish security-related contract terms and service-level agreements. This involves:
   - Validate security terms and conditions in contracts
   - Validate adherence with organization's security and privacy requirements
   - Update contract language based on service and risk level (e.g., right to audit clause, breach notification criteria, points of contact)
   - Establish instructions for return of assets/information upon contract termination

4. Onboarding and access: Stratify third parties into various risk and service categories to create a prioritized third-party security risk register. This involves:

- Third-party access, including risk rating and profile
- Business relationship manager on proper security onboarding activities
- Identify changes to risk rating and profile of third party as part of onboarding, depending on contract terms

5. Monitoring: Periodically assess and monitor third-party security risks and remediation as well as application of appropriate risk treatment and take mitigation steps to address risks arising from the organization's underlying security architecture. This involves:

- Identify changes to risk rating and profile of third party as part of onboarding, aligned with contract terms
- Identify, track, and report remediation and mitigation plans for cyber programs: data loss prevention, identity and access management and system hardening
- Define and report key metrics to management
- Defined events and triggers for post-breach/compromise monitoring

6. Termination: Reassess third-party risk exposure and execute exit strategy, inclusive of revoking all access and return/destruction of assets and data. This involves:

- Confirmed termination of access
- Collection of IT assets and access badges
- Collection or certified destruction of information
- Post-termination monitoring to validate removal of all physical and network third-party access

4 What is not going well?

1. Risk management

The assessment and treatment of information security risks were key challenges across organizations. This includes activities such as the development of an organizational information security risk management methodology, the identification and assessment of information security risks, and the resulting treatment of these risks. (Clause 6.1 of ISO/IEC 27001:2013 refers to information security risk management.)

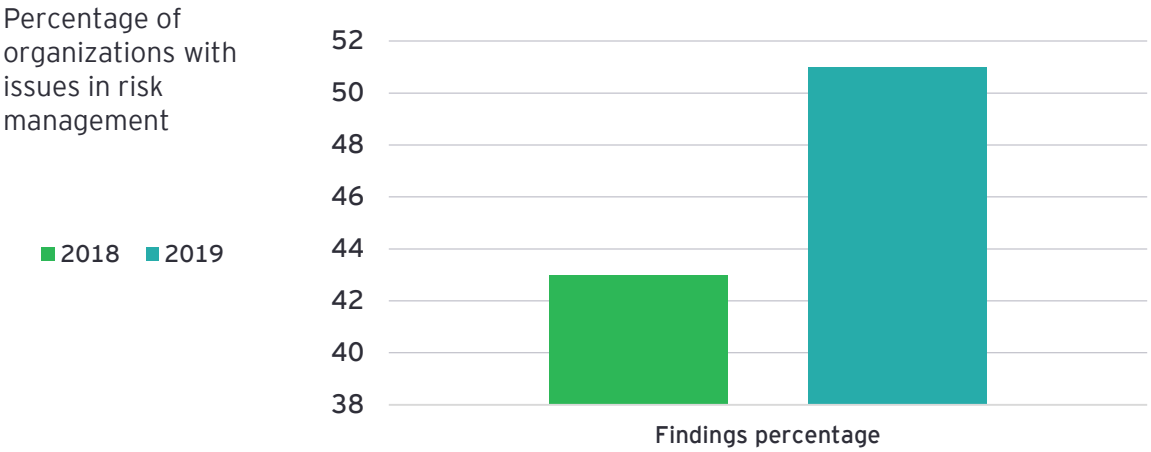
Findings

35%

Findings and improvement areas issued against risk management topics in 2018 and 2019

Risk management is one of the most critical processes to an organization's information security management system. Effective management of risk allows the organization to identify threats and to protect assets and activities in line with organizational objectives while avoiding unnecessary cost.

Risk management must be an ongoing activity so the organization can consider recent developments, both within and beyond the organization, when determining responses to risks.



Source: EY CertifyPoint certification audits

In 2018, 43% of organizations received findings in this area, and in 2019 this figure increased to 51%. This shows that risk management is an increasingly challenging area for many organizations. The distribution of these findings shows that information security risk assessment is a challenge to organizations of all sizes.

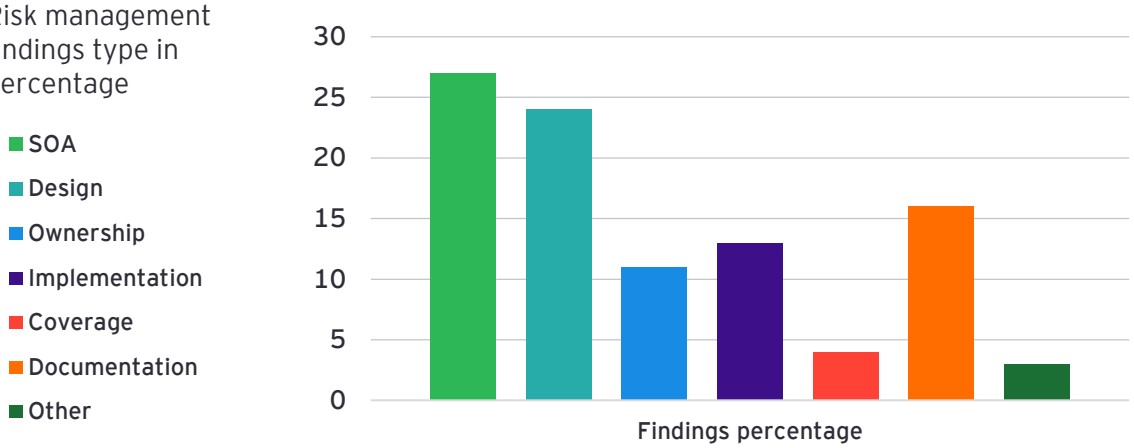
The greatest cause of risk management findings stemmed from the Statement of Applicability (SOA). The SOA is a specific ISO/IEC 27001:2013 document describing which controls from ISO/IEC 27001:2013 Annex A are applicable to the organization along with their justification for inclusion, which controls are not applicable to organization along with their justification for exclusion and the current control implementation status. This critical document is needed for certification audits, and usually customers also ask the organization for this document to assess which of the information security controls are not implemented by the organization for better transparency and trust in the marketplace. The findings were largely documentation errors, so care is needed when determining and documenting the applicability of information security controls to verify that the resulting documentation is accurate.

Risk management must be an ongoing activity so the organization can consider recent developments, both within and beyond the organization, when determining responses to risks.

The second greatest cause of risk management findings was the design of the risk management methodology. A strong risk management methodology can prevent the occurrence of many issues later in the risk assessment process. Therefore, it is important to carefully consider and create the methodology.

Another key challenge within risk management was related to risk ownership. Some of the findings related to the assignment of owners to risks, whereas others were related to the risk owners' acceptance of risk ratings and risk treatment plans.

Risk management findings type in percentage



Source: EY CertifyPoint certification audits

There were also several findings relating to the implementation and documentation of the risk management process. Organizations should take great care when performing and documenting information security risk management activities so they are performed in line with the established methodology and so the related documentation is accurate.

Leading practices for risk management:

- Develop a formal risk management methodology to enable a consistent response to information security risks

The leading practices for designing an information security risk assessment methodology are to:

1. Verify that the method of risk evaluation is suitable for the purpose of the organization. The methodology may be quantitative or qualitative in nature. The main purpose should be to ensure that top management can clearly see the significant risks in the organization so that appropriate measures can be taken.
2. Ensure that the risk assessment design includes how inherent risks (risks without considering controls in place), current risks (risks considering the current implementation status of mitigating controls) and residual risks (future proposed risk values after the additional treatments have been implemented) are calculated.
3. Base the evaluation of risks on the combination of assets, threats and vulnerabilities to identify the critical assets, threats and vulnerabilities that need to be addressed.

4. Confirm that the risk assessment process covers the complete scope of the organization (or certification).
5. Have a feedback loop back to the risk assessment from the performance evaluation (see below), incident management, exception management, etc. processes in the organization to accurately represent the true value of the risks.
6. Design and discuss an appropriate risk appetite so that only less significant risks in the organization may be accepted.

- Further, the risk assessment must include the process of assigning risk ownership in the risk assessment methodology. Please note that the risk owner may be different from the control owner or asset owner. The risk owner should be a person in the organization who can take full accountability of the risks in case the risk were to materialize.

- Ensure that there is a strong and easily identifiable link between the risk management and the statement of applicability.
- Include the process of obtaining risk owner acceptance in the risk assessment methodology.
- Thoroughly review all risk management documentation, including cross-checking linked documents, at regular intervals.
- Formally document and track the implementation status of risk treatment plans: designate ownership, assign due dates and tasks, and regularly follow up on these items.
- Confirm that the risk assessment process produces consistent, comparable and valid results throughout the organization.

2. Performance evaluation

Another area of challenge for organizations was performance evaluation (covered by ISO/IEC 27001:2013, Clause 9). This area includes performance monitoring, ISMS internal audit and management reviews.

Findings

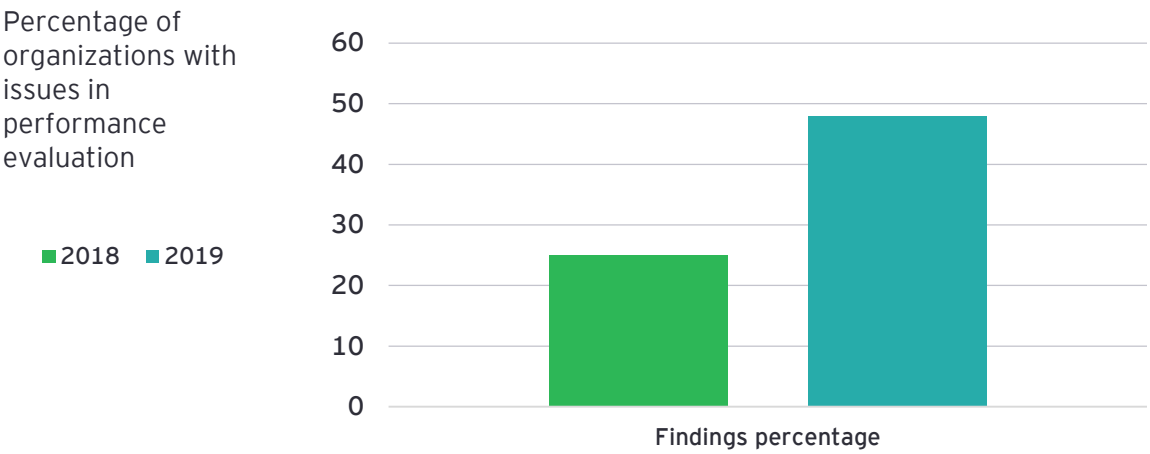
26%

Findings and improvement areas issued against performance evaluation topics in 2018 and 2019

Performance evaluation is important to an effective ISMS, as it allows the organization to identify areas of strength and potential improvement for the ISMS, thus enabling the continual advancement and evolution of the ISMS.

The performance monitoring, ISMS internal audit and management reviews form the three layers of defense in the management system to ensure that the activities are performed in an appropriate manner.

In 2018, 25% of organizations received findings relating to performance evaluation. This rose to 48% in 2019. This significant increase shows that performance evaluation is an area of growing concern and challenge for many organizations.



Source: EY CertifyPoint certification audits

2.1 ISMS internal audit

Within performance evaluation, the area of biggest concern was the ISMS internal audit program (Clause 9.2 of ISO/IEC 27001:2013 provides the requirements for conducting an ISMS internal audit). An effective internal audit acts as a safeguard, allowing the organization to identify issues within the ISMS and address the root causes quickly.

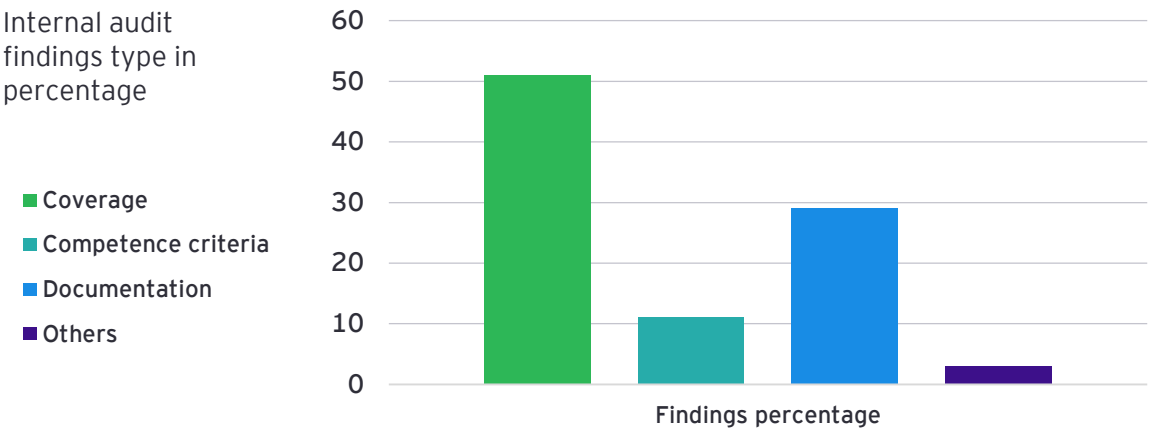
Findings

59%

Findings and improvement areas in performance evaluation issued against internal audit in 2018 and 2019

Within the topic of internal audit, the greatest area of concern was the coverage of the internal audit program.

Organizations must confirm that the scope of the internal audit covers the full scope of the ISMS and assess compliance against all of the organization's information security requirements.



Source: EY CertifyPoint certification audits

The next largest area of concern relating to internal audit was regarding documentation.

These findings typically involved documentation errors relating to the internal audit programs, reports, or the collection and retention of evidence. Organizations should thoroughly and carefully document all internal audit activities to minimize errors.

Another area of concern for internal audits was the documentation and evidence of competence criteria. Organizations should document the competence criteria for personnel performing internal audits, verify that these criteria are met and retain evidence of this.

Leading practices for internal audit:

- Verify that internal audit covers the full scope of the organization (or certification). The internal audit program must cover the management system clauses each year; however, the information security controls may be sampled across multiple years (not more than three years) for adequate coverage. A risk-based approach should be used when defining the audit program for multiple years.
- Ensure that the audit team is independent of the management system processes and controls that are to be evaluated.
- Use auditing techniques to objectively collect and evaluate evidences.

- Confirm that the criteria for selecting internal auditors is defined and followed. Ensuring that the auditors understand the requirements of the standards and the organization's own internal policies and procedures is of utmost importance when selecting auditors.
- Ensure that evidence is appropriately stored and that the conclusions and activities performed during the audit are appropriately documented and communicated to all interested parties.
- Follow up on any findings issued in the previous audits to verify that the root cause of the findings and the corrective actions have been appropriately addressed.
- Ensure that the audit team performs the audit using inquiry, observation and inspection of evidence techniques, with inspection being the strongest method of evaluation. Always corroborate an inquiry in case observation or inspection techniques are not feasible.

2.2 Management review

After internal audit, the next biggest challenge area within the topic of performance evaluation is management review (ISO/IEC 27001:2013, Clause 9.3 lists the requirements for management reviews). Effective management review is important to ensure that top management is aware of ISMS performance and can promote the continual improvement of the management system.

Findings

20%

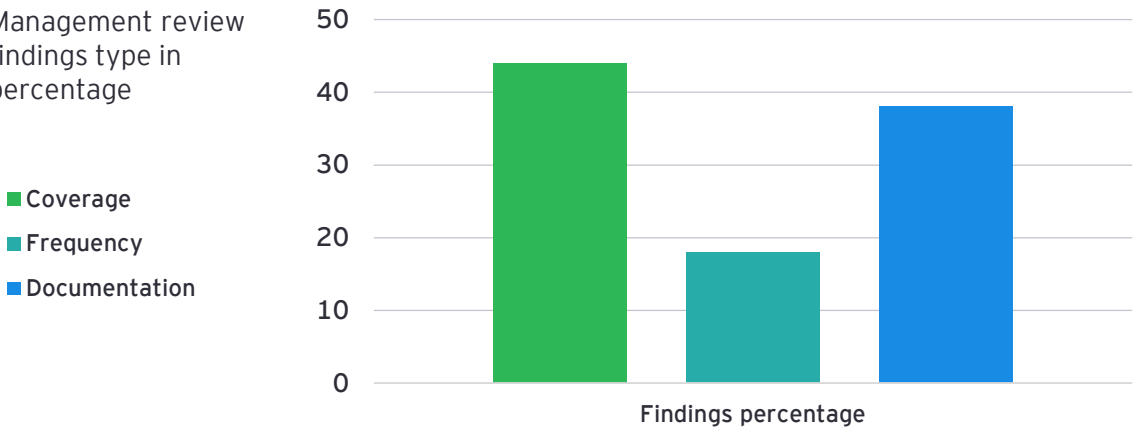
Findings and improvement areas in performance evaluation issued against management reviews in 2018 and 2019

The most significant challenge area for management review was topic coverage. Management review activities must cover certain topics, such as internal and external audit results or the status of activities from previous reviews, in order to be fully informed about ISMS performance.

The next most significant challenge relating to management review was documentation. Management review activities should be carefully documented as either agenda items or minutes of the meeting so top management can follow the progress of the ISMS since previous reviews.

The other challenge for management review was regarding the frequency of management review activities. In order to maintain an up-to-date understanding of ISMS performance, management review activities must happen at least annually. The reviews for all the topic areas do not need to happen in one meeting and can be done regularly to discuss the various topics.

Management review findings type in percentage



Source: EY CertifyPoint certification audits

Leading practices for management reviews:

- Review the full ISMS at least once per year. The management review does not need to happen only once a year, and multiple meetings may be scheduled over the course of the year to discuss various topics.
- Confirm the inclusion of necessary topics, such as audit results, feedback from interested parties, information security objectives, risk assessment and treatment results.
- Clearly define who should attend management review meetings.
- Take formal minutes of meetings and explicitly record any action items. A successful management review does not only include inputs to management but also takes outputs from management at regular intervals.

2.3 Performance monitoring

The other area of performance evaluation is performance monitoring (ISO/IEC 27001:2013, Clause 9.1 defines the requirements for evaluation of the management system and information security controls). This usually entails the development of several KPIs (key performance indicators) relating to information security objectives and/or controls. The set of KPIs often includes both qualitative and quantitative KPIs, with targets defined to track ISMS improvement.

Within performance monitoring, the greatest area of concern was the design of the monitoring. This area includes items such as measurement frequency, the measurement method and the process for responding to the measurement results.

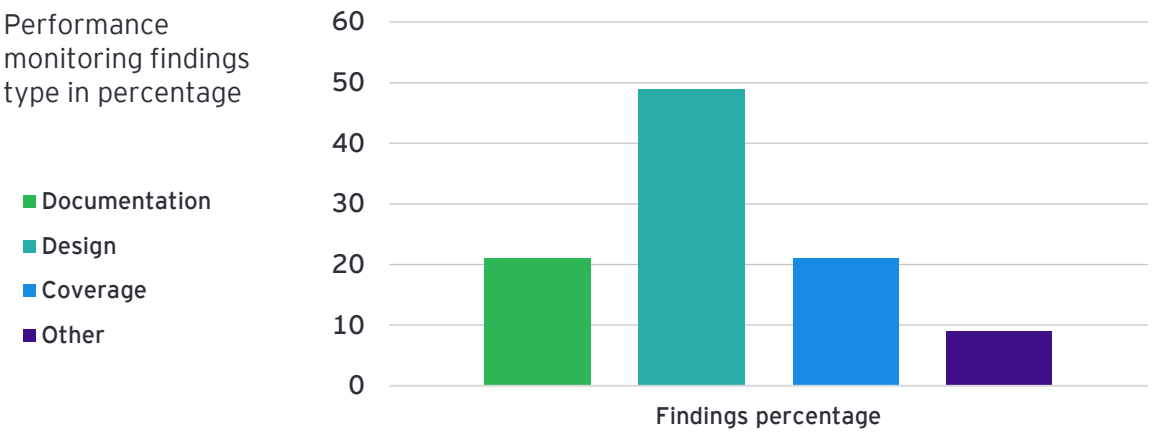
Another area of concern relating to performance monitoring was the coverage of the performance monitoring. KPIs should be developed to sufficiently cover the ISMS to create a comprehensive representation of ISMS performance.

Findings

22%

Findings and improvement areas in performance evaluation issued against performance monitoring in 2018 and 2019

The other main area of concern for performance monitoring was documentation. KPIs and measurement activities should be well documented to allow consistent measurements, which in turn allows ISMS performance to be tracked over multiple years.



Source: EY CertifyPoint certification audits

Leading practices for performance monitoring:

- Design the KPIs to measure both management system performance and information security control performance.
- Cover all areas of the ISMS in terms of the information security controls and objectives.
- Devise the monitoring process to include items such as who will monitor, when will they monitor, how will they monitor and what will they monitor.
- Define targets for KPIs. Review targets at regular, predefined frequencies to continually improve performance. Handle any exception through the audit management process or the nonconformity and root-cause process.
- Perform measurements in accordance with the defined measurement methods and frequencies.
- Retain results of previous measurements to track long-term changes.

3. Scope of ISMS

The next key area of concern was the scope of the ISMS. Most of the findings on this topic related to the documentation of the scope. The scope of an ISMS must be carefully and comprehensively documented so that areas that must be protected are not accidentally excluded from ISMS activities.

Findings

12%

Findings and improvement areas issued against the scope of ISMS in 2018 and 2019

In 2018, 11% of organizations received findings related to this area, and in 2019, this figure rose to 21%. This sharp increase shows that scope of ISMS is an area of growing challenge and concern across industries.

Please see Section 3 ‘Trends in scope changes’ for further details around how the scope has increased in terms of both locations and employees in-scope.

Source: EY CertifyPoint certification audits

Leading practices for ISMS scope:

- The scope of the information security management system should only be defined once the context of the organization and the interested parties are clearly understood. The context of the organization maybe understood by looking at both internal and external factors, such as the organization's industry, locations and culture. The interested parties are the parties that may have a vested interest in the performance of information security and cybersecurity operations of the organization and may include customers, employees, regulators, trade groups, competitors, media, etc. The requirements of such interested parties must be known and the scope of the management system must be defined to cover these requirements.
- The ISMS scope should include the locations, employees, products and services, departments and functions, IT assets, etc. that are in scope of the management system.
- Explicitly list all of the interfaces and dependencies that may impact the ISMS. The interfaces and dependencies are the areas that are not in scope of the management system but may be activities, processes, teams or other organizations that may impact the performance of the management system. Such interfaces and dependencies should be monitored regularly.
- If any locations or functions are excluded from scope, document the justification for this and regularly review whether this justification still applies.
- Regularly review the scope document to confirm its continued validity.

- For onboarding new locations, employees, departments, products, etc. into the management system, make sure that the new area to be onboarded is covered in the risk assessment and treatment process, the KPIs have been defined and assigned, the internal audit has been performed, the management review is completed, any findings or deviations have been sufficiently handled through the correct process, all information security controls have been designed and implemented appropriately, and there is adequate budget and resources to continually operate the new area as part of the management system.
- For onboarding new entities/companies or for new mergers and acquisitions:

  A. Before merging the IT systems:
  - Identify what types of cyber risks the target company faces based on its industry, geography, partners, products and services.
  - Study network and system architectures, including known hardware and software vulnerabilities, IT and OT asset inventory, patching schedule, digital asset management, cloud services, mobile policies, application vulnerabilities, data flows, and more.
  - Understand all data-handling measures, data privacy and security controls, including how the acquisition stores, uses and disposes customer data. Review any contractual obligations, specially over data, that the acquired company may have with another company.
  - Review the acquired company's security program to verify that it meets contractual and regulatory requirements, current industry standards, and leading practices in the industry.
  - Review the existing security policies and audit results with respect to processes (operations), people and technology.
  - Investigate any previous complaints or litigation around fraud, extortion, ransom, etc.

  B. Assess M&A security:
  - Review common organizational policies, including the information security policy, terms of use agreements, acceptable use policy and data classification policy.
  - Consider the results of previous security audits and assessments, vulnerability scans and penetration tests when formulating incident response plans and playbooks.
  - Network segmentation and network policies, which are crucial to realizing the synergy of the acquisition.
  - Review the acquired company's risk strategy.
  - Examine the state of Internet of Things (IOT) security (if applicable).

  Other M&A security factors to consider include IT security expenditures, future cybersecurity plans, certifications, regulatory compliance, cyber insurance policies, employee background verification and off-boarding, security operations centers (SOCs), cybersecurity awareness programs, vendor risk assessments, authentication and access controls, encryption, network monitoring, disaster recovery and business continuity planning, organizational structure, and the information security reporting chain.

C. Post-assessment activities include:

- Map the available systems and processes according to the ISMS and the plan, do, check, act (PDCA) cycle that the organization follows.
- If the acquired company is not technologically mature, it may be prudent to employ a third party to conduct an independent security audit, which includes vulnerability scans, penetration tests and custom methods, to assess the security posture of the acquired company.
- Evaluate IT security personnel through security questionnaires and interviews to help security and business leaders distinguish between competent employees and weak links, if any.
- During and post-merger, implement granular controls for identity and access management (IAM), harden perimeter security and audit logs, and revise security processes and cybersecurity training.

4. Access management (identity and access management)

In terms of information security controls, the biggest challenge for organizations was access control (ISO/IEC 27001:2013, Annex A, Domain A.9 defines the information security controls for access management). Effective access control is vital to strong information security, as it prevents the unauthorized use of or access to information assets.

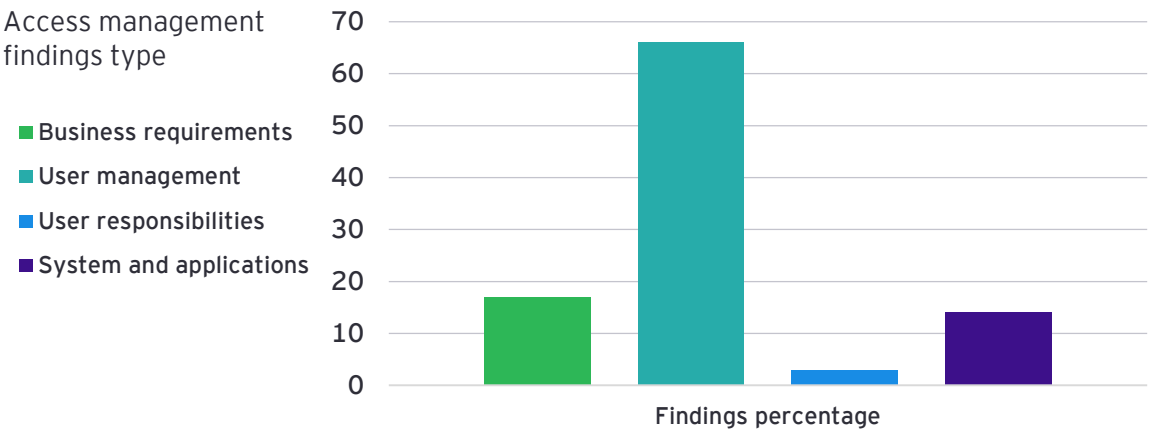
Findings

16%

Information security control findings and improvement areas issued against access management topics in 2018 and 2019

Within this topic, findings are categorized into four subdomains: business requirements, which includes high-level controls such as an access control policy; user access management, which includes user-focused controls such as reviews of access rights; user responsibilities, which includes users' responsibilities for access control; and system and applications, which includes system and application level access controls

The number of findings relating to access control increased by 56% from 2018 to 2019, which shows that this is an area of increasing challenge to organizations. The increase was highest for large-scale organizations.



Source: EY CertifyPoint certification audits

Within the area of access control, the greatest challenge was user access management, specifically access reviews and the removal of access. Organizations should review access rights regularly to verify that access rights reflect current requirements. In line with this, organizations must revoke or adjust access rights appropriately when no longer needed (for example, when an employee's employment is terminated or changed).

Findings

56%

Increase in information security control findings and improvement areas issued against access management topics in 2018 and 2019

Leading practices for access control:

- Centralize the approach: Because identities must be defined when a user is onboarded into a network and managed throughout the user's life cycle, businesses must select a reliable centralized option with strong security. Active Directory is a common choice for managing all network identities in one place, but the possibility of using blockchain technology to create, verify and store unchanging identities in a protected neutral environment may become a reality in the near future.

- Zero Trust identity security: Zero Trust states that enterprise IT security shouldn't trust any user or application under any circumstances. An enterprise shouldn't trust anything trying to connect to its network and databases and thus constantly verifies its legitimacy before granting access.
- The principle of least privilege: This states employees should only possess the permissions necessary to perform their job processes. Yet role-based access focuses on identity governance, whereas the principle of least privilege focuses on initial permissions granted.
- Automate provisioning: Entities need to manage new users, users who leave the organization, and users who move or are promoted or demoted within the organization. Provisioning, de-provisioning and re-provisioning are often time-consuming, manual tasks, and automating them can not only reduce overhead but also reduce errors and improve consistency.
- Check and recheck: Permissions require periodic recertification — reviewing who has access to what and determining whether or not they should still have those permissions. Define job roles within an organization that can recertify permissions, such as system owners, managers and information security officers. Recertification can be defined in a workflow in which data owners and custodians review a current permission set and verify the accuracy (or inaccuracy) of that set. The idea is to regularly confirm that the roles and people who have permissions to resources should continue to have those permissions.
- Pinpoint and eliminate high-risk systems: Despite the wide availability of cloud-based frameworks and applications, many businesses are still clinging to legacy systems for which support has long since ceased. Unpatched systems can become sources of data leaks and make sensitive information readily available to hackers.
- Multifactor authentication: Passwords, the foundation of most single-factor authentication schemes, consistently prove unreliable for enterprise identity security. Hackers of even nominal skill can easily crack, guess or circumvent password-based logins. Therefore, the enterprise needs to deploy and maintain multifactor authentication as part of its access management leading practices. The more steps between the access request and the digital assets implemented, the more secure they remain. Multifactor authentication steps can include biometrics, geofencing, time of access request monitoring, hard tokens, SMS messaging systems and even passwords. If employees find multifactor authentication an impediment to their business processes, one can weigh the prospect of step-up authentication instead.
- Crack down on orphaned accounts: Active user accounts contain all the information related to a user's identity and the person's movement within a network, including access privileges. When a user is promoted to another position or leaves the company, these accounts should be removed. However, with the increasing burden on IT professionals and the lack of visibility in most business networks, this often does not happen. Improper de-provisioning of users leads to an accumulation of accounts with no associated users.

5. Asset management

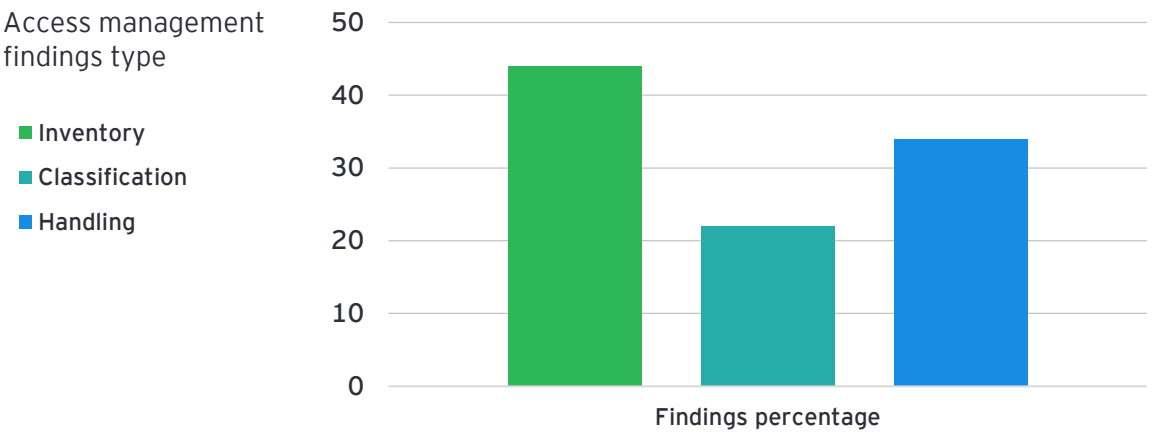
Another control domain that was a challenge for organizations was asset management (ISO/IEC 27001:2013, Annex A, Domain A.8 provides the controls for asset management). Findings relating to asset management changed by less than 2% from 2018 to 2019, showing that this is an area of consistent challenge for organizations. Asset management is a key domain for an ISMS because an information asset can only be protected if it is carefully managed.

Findings

13%

Information security control findings and improvement areas issued against asset management topics in 2018 and 2019

Within the domain of asset management, the most significant challenge was the asset inventory. An asset inventory is critical to the performance of the ISMS as it allows the organization to identify information assets and their current status. This inventory can then be used to inform other ISMS functions such as the risk assessment.



Source: EY CertifyPoint certification audits

The next most significant challenge was around information classification, which ensures that users and systems are aware of how information of varying sensitivities should be treated.

The other key challenge in the domain of asset management was media handling. This area refers to the handling of physical media storing information and is important as it prevents logical security controls from being bypassed physically.

Leading practices for asset management:

- **Asset repository**: An effective IT asset management (ITAM) function should include an IT asset management repository, data on both hardware and software components, and a set of processes for maintaining that data. At the most basic level, an ITAM function must be able to discover all hardware and software components in the IT environment and record them in the asset management system. As new components are introduced, they are added to the asset inventory. Data capture includes identifying both the object and the supplemental information that supports decision-making. It is important to know possible about an organization's assets. Management must capture as much asset information as possible to help drive critical decisions during the future. The first step is to discover the assets in the IT environment. There are many methods to identify IT assets, including:
  - Manual audits
  - Reviewing procurement records
  - Agent-based discovery tools
  - Agentless discovery tools
  - Change management records

  Each of these methods has advantages and disadvantages. Selecting the right method for an organization's unique needs requires a clear understanding of the data it is trying to capture, the types of components in its IT environment and how current the data must be. Automated approaches are often much quicker and provide more accurate and real-time data but are prone to missing unexpected assets. Manual processes are more likely to encounter asset exceptions but can be costly and time-consuming to perform (a manual-asset audit in a data center may take weeks).

  Leading practices suggest the best way to inventory assets is to use a combination of multiple techniques for a balanced perspective of both breadth and depth.

- **Keeping inventory up to date**: IT asset data comprises two components: a lists of items and the relationships between them. Capturing relationships is equally (if not more) important than capturing the lists. Many companies have found that focusing on dependency mapping is a more effective method to identify meaningful information about assets than discovery tools that focus only on capturing lists of assets (and associated attributes).

This is because dependency relationships provide insights into two or more assets (instead of just one) and provide the context of why the assets are connected. The context information is essential for making informed asset-management decisions.

- A configuration management database (CMDB) is a virtual replica of an organization's IT environment. It is the repository where management should store all asset-related data. By using the CMDB effectively, asset information will not only be available to support ITAM processes but also easily accessible to other IT service management (ITSM) processes (e.g., incident and change management) that must access it.
- The biggest challenge of IT asset management is keeping asset records updated as the IT environment evolves. Business decisions, system upgrades, new technology developments and users changing job roles can all have an impact on how assets are used and the value they create for the organization. Some of these changes can be captured through ITSM workflows, such as change management and release management, while capturing other changes (such as business reorganizations) requires surveying the broader environment where IT assets operate.

- **Keeping inventory complete and accurate**: Leading practices suggest that to keep IT asset data complete, accurate and current, companies should leverage a combination of automated-discovery capabilities, workflow triggers and periodic manual reviews. The five key change management activities that should be included in an ITAM program include:
  1. Assessment of new assets — Whenever a new asset is added to the IT environment, it is likely to impact the use of other assets. Workflow triggers in the procurement-and-provisioning processes can alert management to the introduction of new assets, and these events can then be correlated with changes observed in monitoring data.
  2. Periodic review of asset utilization — Operational-monitoring capabilities provide real-time insights into the usage of IT assets. Some companies have even implemented telemetry that shows what users are accessing a system and/or what functions or workflows they are using. Changes in asset utilization are indicators that something has occurred in the business environment that could impact the ROI (return on investment) or life cycle of the asset.
  3. Identifying missing assets — It is important to maintain records of assets' intended use and who is assigned to use them. This is particularly true with components such as desktops, printers, phones and other IT assets that are easily moved. While asset theft is a problem, an even bigger challenge is unauthorized re-provisioning of assets without informing the IT department. Missing assets that have been moved or re-purposed can lead to significant maintenance costs and security risks during the future.
  4. Reviewing software licenses and subscriptions — Software licenses should be reviewed regularly to ensure the company is neither overpaying for unused resources or using software that isn't covered by a valid license or subscription. Since most software licenses must be renewed periodically, aligning asset-record updates to the renewal cycle is often effective.

5. Tracking asset changes — Identifying and tracking changes of the location of assets can increase or decrease the number of assets, change asset use, and update the asset's life cycle status. IT environments are constantly changing, and IT asset records require continuous updates to remain current and accurate.

- **Asset life cycle management:** Tracking an asset's life cycle ranges from requisitioning, purchase and assignment to retirement and decommissioning. The value of an asset changes throughout its life cycle, so maintaining current life cycle data is key to asset efficiency.

  Each asset progresses through a series of life cycle stages from the time it is procured and provisioned through use and upgrades, eventually ending with retirement and either removal or replacement. Companies may define life cycle stages in different ways or using different terms, but IT asset management leading practices suggest a company should have a clearly defined asset life cycle that is used consistently throughout its IT organization:
  - IT asset management policies and processes should be tied to asset life cycle stages. These might include a set of policies and processes about what assets can be procured and introduced into the IT environment. Or an organization might have separate processes for managing upgrades and making changes to assets' uses. Policies and processes are the tools for driving efficiency, transparency and value throughout the asset life cycle.
  - It is important to track the complete life cycle of assets. Many companies struggle with this task. As an asset progresses through its life cycle, different teams may be involved in making decisions about it, and asset records may be present in multiple IT systems. Effective IT asset management requires gathering all the asset management life cycle components into an integrated set of processes and a consistent set of data. This enables big-picture visibility and the data needed to drive management insights critical to decision-making.
  - Another important life cycle management activity is tracking the state of assets carefully — verifying that any change in an asset's status, its use or the costs it is incurring is reflected in an IT asset management repository. An IT environment has several forces that can impact the cost and potential value of an asset. Informed decision-making requires complete, current and accurate asset data.

- **Asset reporting and alerting:** Generating asset inventory reports and alerts on asset changes and life cycle-related activities that require attention. IT asset management can help drive decisions, not just support them. IT asset management is a data-driven activity. Much of ITAM's focus is creating and managing asset data; however, it is the consumption of ITAM data to support decision-making where an organization reaps the benefit from its various ITAM investments. Both raw asset data and curated metrics are important in providing IT leaders the big picture and actionable details needed to make decisions about how to employ IT assets effectively.

Each IT organization will have a unique set of data and metric needs based on the types of questions leaders are trying to answer. The metrics themselves are less important than the usefulness of the information to drive actual decisions. Often, ITAM programs start either without any specifically defined objectives or with a long list of metrics leaders think should be tracked without any actual idea of the metrics' use. IT asset management leading practices suggest companies should leverage metrics and reports that are included in the box with their ITAM software as a starting point, and then define additional organization-specific metrics and reports to address specific operational or decision-support needs.

Companies should also leverage three different types of data views to support IT asset management. Each of these types of data views provides a unique perspective of the IT asset landscape and ITAM processes. Selecting the right view can make a big difference in the usability of data:

1. Dashboards provide real-time snapshots of asset data and are useful for ITSM processes, such as incident and change management.
2. Reports aggregate data during time intervals to show trends, groupings and high-level overviews of assets and their use.
3. Raw data is necessary for integrating with other IT systems and supporting deep analytics of IT asset data to support specific decision-making or project needs.

It is important that companies establish specific goals/issues they want their ITAM program and supporting projects to address. Without being able to clearly articulate the goals a company is trying to achieve, it is difficult to identify which metrics will be most effective in helping achieve those goals. For continuous ITAM programs, exception reports are also a very useful tool. Sometimes, exceptions to processes and unusual data provide the most meaningful and actionable improvement insights.

6. Physical and environmental security

The last control domain that was a challenge for organizations was physical and environmental security (ISO/IEC 27001:2013, Annex A, Domain A.11 provides the controls for managing physical and environmental security). This domain is crucial to the performance of an ISMS, as technological controls can often be easily bypassed by an attacker with physical access to an asset.

Findings

7%

Information security control findings and improvement areas issued against physical and environmental security topics in 2018 and 2019

Within this domain, the biggest challenge was the clear desk and clear screen policy. This is a key control as it reduces the chance of an unauthorized person viewing sensitive information, either on an authorized user's screen or as a paper copy on a desk.

Source: EY CertifyPoint certification audits

Another key challenge area was the siting of equipment. Equipment must be placed in an appropriate location to reduce the risk from both environmental and malicious threats and hazards.

The next largest area of concern was physical access controls. Physical access to areas containing sensitive information assets should be restricted to authorized personnel.

Leading practices for physical and environmental security:

- Include clear desk and clear screen requirements in all information security awareness materials and trainings.
- Perform regular office walks to monitor compliance with clear desk and clear screen policies.
- Determine which managers are responsible for planning, funding and operations of physical security of the data centers and/or office locations or any other locations in scope of the management system.
- Determine whether an appropriate investment in physical security equipment (alarms, locks or other physical access controls, identification badges for high-security areas, etc.) has been made and if these controls have been tested and function correctly.

- Establish a baseline by evaluating the gaps in physical security controls, which will include the following as they relate to a company's locations:
  - Environmental controls
  - Natural disaster controls
  - Supporting utilities controls
  - Physical protection and access controls
  - System reliability
  - Physical security awareness and training
  - Contingency plans
- Provide responsible managers guidance in handling risks. For example, if the current investment in physical security controls is inadequate, this may allow unauthorized access to servers and network equipment. Inadequate funding for key positions with responsibility for IT physical security may result in poor monitoring, poor compliance with policies and standards, and overall poor physical security.
- Maintain a secure repository of physical and environmental security controls and policies and establish timelines for their evaluation, update and modification.
- Create a team of physical and environmental security auditors, outside of the management staff, to periodically assess the effectiveness of the measures taken and provide feedback on their usefulness and functionality.
- IT equipment should be maintained properly and disposed of securely. Information stored in equipment being disposed, redistributed or sold must be securely removed to prevent the disclosure of the information to unauthorized parties.
- The system's operation usually depends on supporting facilities such as electric power, heating and air conditioning, and telecommunications. The failure or substandard performance of these facilities may interrupt operation of systems and cause physical damage to system hardware or stored data. Equipment should be protected from disruptions caused by failures in supporting utilities such as HVAC, water supply and sewage. Power and telecommunications cabling carrying sensitive data should be protected from interception or damage. Maintenance contracts should be in place to properly maintain equipment to enable its continued availability and integrity. Equipment, information or software should not be taken off-premises without prior authorization. Appropriate security measures should be applied to off-site equipment, taking into account the different risks of working outside the organization's premises.
- There are many types of equipment involved in the creation, collection, storage, manipulation and/or transmission of information. Filing cabinets store student transcripts. Computer systems process and maintain intellectual property. Data networking equipment and cables transmit voice and video communications. While the value of the equipment cannot be disregarded, the information stored in the device is arguably more valuable than the device itself. Physical and logical security safeguards should be based on the type of data being processed by the equipment. A sound asset management strategy is important to track and appropriately secure all important equipment.

- All equipment containing storage media should be checked to confirm that sensitive data and licensed software have been removed or securely overwritten prior to secure disposal.
- In the event that equipment is lost or stolen, a number of steps must be taken. Immediately inform the information security office (or those responsible for information security in the institution) of the loss. Providing as much information as possible about the contents (social security numbers, credit card numbers, protected health information, personally identifiable information, etc.), use (e.g., passwords on the device that could be used to access secure institution resources) and life cycle (has the device been shared with others, has it been scrubbed recently of data within, etc.) of the stolen property is essential to determining the risk involved and the required actions involved in its recovery or remote wiping of data housed. Identification of IP addresses, hostnames, computer names registered or other associations with the stolen property provides additional information leading to its return or calculating the impacted loss. Evidence that the device is registered with a device management system (mobile management system, online location service, etc.) may enable the risk to be mitigated without the device's recovery. Confirmation that the device is encrypted or backed up also affords data relative to its risk of loss to the institution. Finally, have police been informed of the theft or loss in order to file appropriate reports for insurance purposes or data loss prevention activities.
- Physical security begins with low visibility for secure locations. Unnecessary signage announcing high-impact data facilities and network closets should be avoided. Mechanical locks with different keying options, some of which allow multiple key codes for added security, are turning to electronic access solutions with entry audit capabilities. Complete access solutions, consisting of electronic access control devices and remote monitoring capabilities, are becoming more prevalent where access is granted to multitudes of people throughout the day. Fully networked RFID (radio-frequency identification) and biometric readers provide additional security where ID cards can be shared, lost or stolen.
- Electronic access solutions eliminate managing multiple keys and provide real-time remote access monitoring and audit trail reporting, meeting compliance requirements where required. Electronic access reporting can provide simple open/close information as well as additional data involving which credential was used, the time and duration of the event, and the type of access activated. In the event a security breach does occur, the audit trail can be used to forensically reconstruct a series of events leading up to the suspicious activity.
- Networking security access keep equipment and spaces secure, connecting building security and equipment access through standardized security credential protocols. Electronic locks can communicate with IP security cameras or other security devices, expanding the scope and capabilities of a security network.

- Naturally limiting access to secure spaces is the best method of controlling the security of those facilities. Only those who absolutely need access should be among those granted that permission. Most technology can be managed remotely without actual physical access to the equipment. Where physical access is determined necessary, that access should be monitored, recorded and audited absolutely.
- Fire, humidity, smoke and temperature control systems are all available, which can provide monitoring capabilities and automated activity including alarms, fire suppression and alerts. These should all be deployed to keep systems operating, with appropriate training (use of gas masks, fire extinguishers, emergency power shutdown management systems, etc.) provided for those responsible for their maintenance and safety.
- All of these systems and processes can be implemented over time but should be part of a physical security system for technology. Relatively inexpensive, the assurance that equipment housing essential institution data is safe and secure is well worth the cost.

7. Privacy accountability

From a privacy perspective, the greatest challenge area was accountability (ISO/IEC 27018:2014, Domain A.9, provides controls for privacy accountability when processing PII on public cloud services). This area includes topics such as the notification of PII principals in the event of a data breach; the retention of security policies and operating procedures; and the return, transfer and disposal of PII.

The area of accountability is increasingly important in the context of privacy, as organizations processing PII must build trust with increasingly wary PII principals. Findings in this area grew by 20% from 2018 to 2019, which suggests that privacy accountability is an increasingly challenging area for organizations that process PII.

40%

Findings

Findings and improvement areas related to privacy and accountability in 2018 and 2019

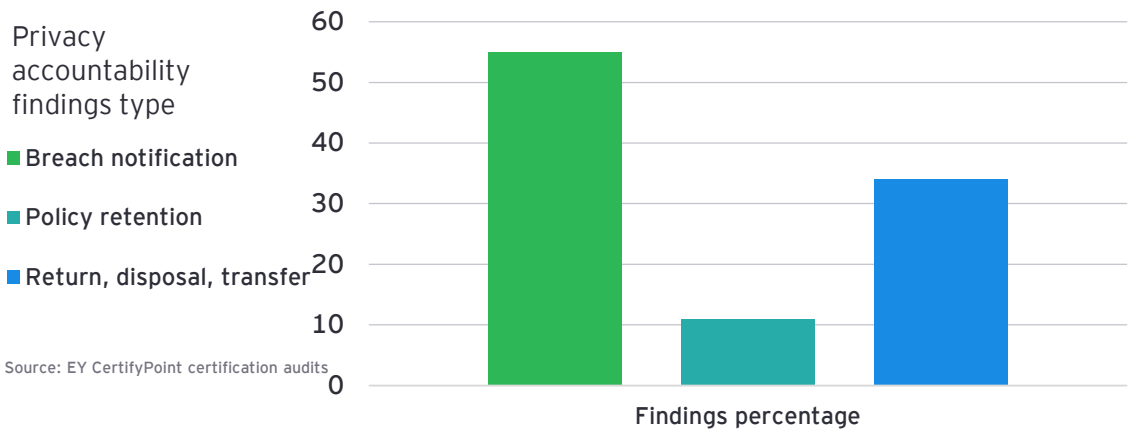
20%

Findings increase

Increase in findings from 2018 to 2019 for the topic of privacy and accountability

Within the area of accountability, the topic of most concern is the notification of PII controllers in the event of a data breach. This is an important control, as it alerts PII controllers and principals in due time of any potential data breaches that may have leaked personal information.

Timely notification from the processors is critical and must be established according to local privacy laws such that controllers and principals can inform and take due action as appropriate.



Source: EY CertifyPoint certification audits

The other challenge within this area is the return, transfer and disposal process for PII. It is critical that PII be protected once it is no longer required. The organization must ensure that the PII is returned to the PII controller, transferred to another organization or securely destroyed.

Policy retention is the retention of previous versions of policies after the policy is updated. This allows an organization to identify what their internal policy requirements were at a certain point in time, which may be necessary for some customer dispute resolutions or PII protection investigations.

Leading practices for privacy accountability:

- For data breach notifications, leading practices include:
  - Have a written data breach response plan
  - Designate a team to coordinate the response
  - Hold desktop incident exercises to test the plan
  - Develop internal notification procedures
  - Conduct initial investigation and take risk reduction measures
  - Make the decision whether to notify:
    - Notification: Identify whom to notify (potentially including law enforcement, government agencies, affected individuals); timing, method, contents and format of notice
  - Conduct final assessment (lessons learned, corrective measures and policies, changes to response plan

- For policy retention, leading practices include:
  - Create retention scheme for security policies and guidelines
  - Set retention period (five years after update recommended)
  - If possible, use an automatic tool to ensure compliance with this retention period

- For return, transfer and disposal of data, leading practices for formulating a policy include:
  - Take into account the right of principals to access and delete their data at any point
  - When transferring data from one country to another, follow local and internal laws and establish appropriate security controls when transferring such data
  - When transferring the data from one controller to another or from one processor to another, follow the guidelines as stipulated in the contracts:
    - Contracts with controllers or processors (as applicable) should encompass the minimal technical security measures and methods that would be undertaken in case of transferring data from one organization to another.
  - For each processing and controlling activity, define an archival period:
    - Archive the old data according to the defined timelines
    - Delete old data once this archival period is over from all places (applications, databases, network devices, paper, emails, etc.)

5 Further EY insights

What have we seen so far in 2020?

Risk management continues to be a challenge for organizations. As of 30 April 2020, we have seen nearly 45% of management system findings issued against risk management. Although there are significant number of findings against risk management, we have seen an ever-increasing maturity in the design and implementation of risks in organizations where automated tools, executive-level dashboards and streamlining of processes have aided in simpler yet extensive risk analysis.

Findings

45%

Findings and improvement areas for management system related issued against risk management topics in 2020 (through 30 April 2020)

Another area where organizations are continuing to fail is IT asset management. We have so far in 2020 seen nearly 17% of the findings in control areas being toward ITAM. With the impact of COVID-19 crisis, organizations have been tackling other key areas of interest to minimize workforce disruption and business continuity. IT asset management seems to have been put so far to a lower priority on the executives' agenda as they strive to ride out the immediate short-term repercussions of the pandemic.

An area that seems to have improved is physical and environmental security, where no findings have yet been issued. This is due to the COVID-19 pandemic's impact, where travel advisories across the globe have changed the normal course of audit operations. Organizations, regulators and auditors are now relying on compensating mitigating controls to evaluate physical and environmental threats and their effect on the workforce and the organization's processes.

A new topic of concern in 2020 so far has been on operations security (ISO/IEC 27001:2013 provides requirements from an operational security perspective). Operational security includes change management, backups, protection from malware, logging and monitoring, etc. We believe that the higher number of findings issued against this control domain has also been due to the impact of COVID-19 pandemic as organizations are adapting to the new ways of working, focusing and readjusting their existing IT operations to more digital ways.

Findings

15%

Information security control findings and improvement areas issued against operational security in 2020

As we all tackle the pandemic together, it remains unclear how the cybersecurity sphere will adapt to the new norms and how executives and organizations will collaborate to manage information security and cybersecurity in their organizations. It is also difficult to predict what new leading practices shall be the new norm going forward and what role emerging technologies, such as artificial intelligence and blockchain, will play in the next decade.

Appendix - About the standards

ISO/IEC 27001:2013 (information security management system)

The purpose of ISO/IEC 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements*, is to provide a set of requirements against which information security management systems (ISMS) can be audited and certified. ISO/IEC 27001:2013 is written to enable all organizations to establish, implement, maintain and improve an ISMS, rather than focusing on specific sectors or types of organization.

An information security management system is a systematic, risk-based approach for establishing, implementing, monitoring, reviewing, maintaining and improving an organization's information security to achieve business objectives.

The standard structure is composed of:

A. Three introductory clauses:

1. Scope
2. Normative references
3. Terms and definitions

B. Six management system clauses, which describe the requirements for implementing and operating the ISMS:

4. Context of the organization
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance evaluation
10. Improvement

C. Annex A, which is a list of controls that organizations may implement according to their requirements. These controls are also listed as clauses in ISO/IEC 27002:2013. They are organized into 14 control domains:

A.5 Information security policies
A.6 Organization of information security
A.7 Human resource security
A.8 Asset management
A.9 Access control
A.10 Cryptography
A.11 Physical and environmental security
A.12 Operations security
A.13 Communications security
A.14 System acquisition, development and maintenance
A.15 Supplier relationships
A.16 Information security incident management
A.17 Information security aspects of business continuity management
A.18 Compliance

ISO/IEC 27017:2015 (information security controls for cloud services)

The purpose of ISO/IEC 27017:2015, *Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*, is to provide additional information regarding security controls and requirements for cloud service providers and cloud service customers.

This standard consists of two main sections. The first provides additional requirements for the controls from ISO/IEC 27002 (or ISO/IEC 27001:2013 Annex A) for both cloud service providers and cloud service customers. The second provides seven additional controls relating to information security in cloud services:

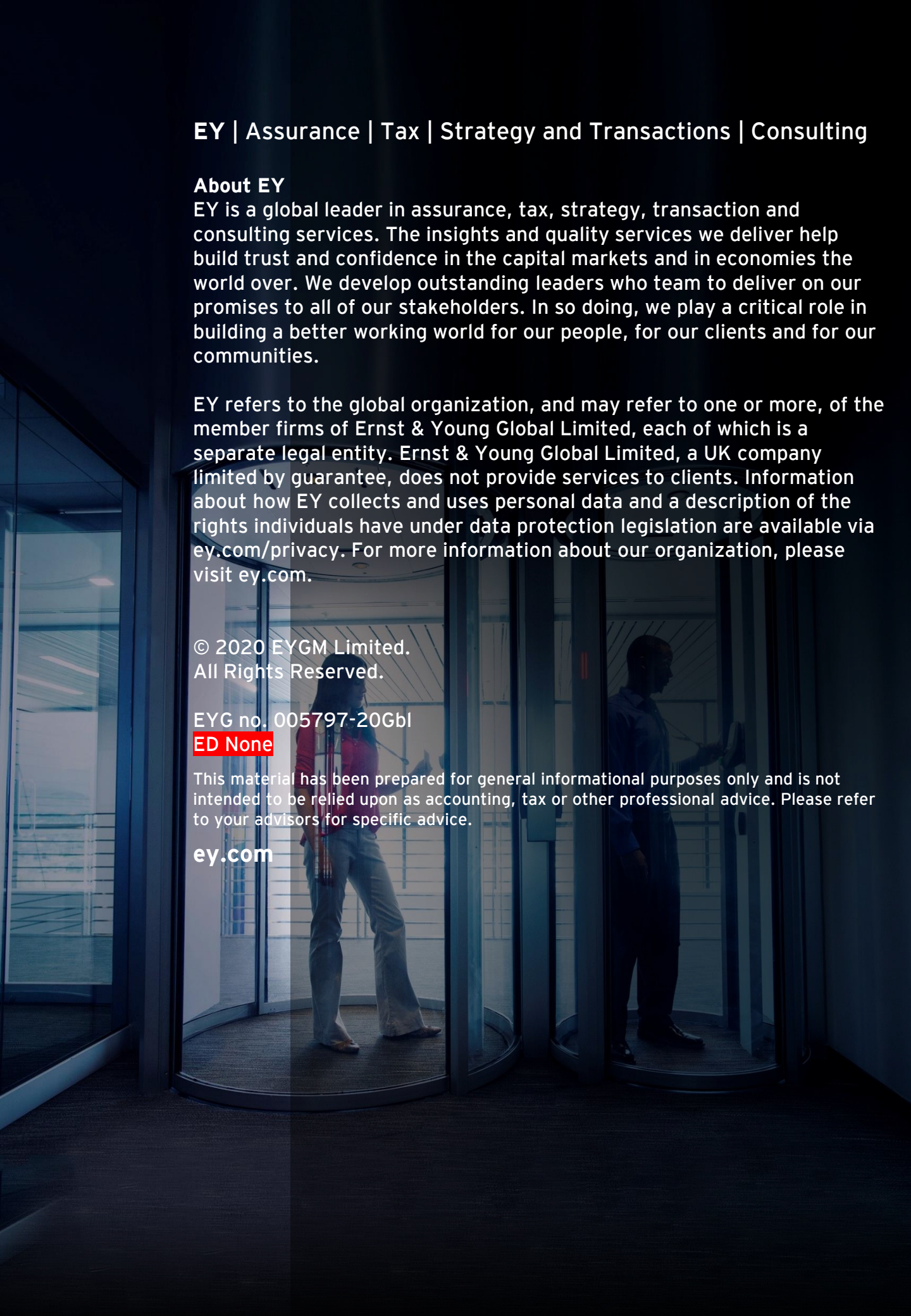
- CLD.6.3.1 Shared roles and responsibilities within a cloud computing environment
- CLD.8.1.5 Removal of cloud service customer assets
- CLD.9.5.1 Segregation in virtual computing environments
- CLD.9.5.2 Virtual machine hardening
- CLD.12.1.5 Administrator's operational security
- CLD.12.4.5 Monitoring of cloud services
- CLD.13.1.4 Alignment of security management for virtual and physical networks

ISO/IEC 27018:2014 (information security controls for protection of personally identifiable information (PII) in public clouds acting as PII processors)

The purpose of ISO/IEC 27018:2014, *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*, is to provide additional controls and requirements for the protection of PII in cloud service environments.

The structure of ISO/IEC 27018:2014 is similar to ISO/IEC 27017:2015. It consists of two main sections, the first of which provides additional requirements for the controls from ISO/IEC 27002 (or ISO/IEC 27001:2013 Annex A), while the second provides 11 additional privacy protection control domains:

- A.1 Consent and choice
- A.2 Purpose legitimacy and specification
- A.3 Collection limitation
- A.4 Data minimization
- A.5 Use, retention and disclosure limitation
- A.6 Accuracy and quality
- A.7 Openness, transparency and notice
- A.8 Individual participation and access
- A.9 Accountability
- A.10 Information security
- A.11 Privacy compliance



EY | Assurance | Tax | Strategy and Transactions | Consulting

About EY
EY is a global leader in assurance, tax, strategy, transaction and consulting 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. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. For more information about our organization, please visit ey.com.

EYG no. 005797-20Gbl
ED None

ey.com