Organizers

Sponsor

Report on Hong Kong SME Cloud Adoption, Security & Privacy Readiness Survey

Produced by Internet Society Hong Kong and Cloud Security Alliance (Hong Kong & Macau Chapter)

Sponsored by Microsoft Hong Kong

Compiled by
Internet Society Hong Kong
Cloud Security Alliance Hong Kong and Macau Chapter

Oct 25, 2017

Organizers

Sponsor

Table of Contents

Organizers

Sponsor

Executive Summary

In March 2017, the Internet Society Hong Kong (ISOC HK) and Cloud Security Alliance – Hong Kong and Macau Chapter (CSA HKM), with funding sponsorship from Microsoft (HK), jointly conducted the Hong Kong SMEs Cloud Adoption, Security and Privacy Readiness Survey. We have received feedback from and interviewed 103 local SMEs coming from various industries including retail, manufacturing, Information and communications, imports/exports, financial services, etc.

This is the third survey and the survey **scope has been expanded this year to cover the preference of Cloud Service Providers** (CSPs). Comparisons done against last survey's data have also provided valuable insight on the progress of Cloud adoption status in SMEs.

The questionnaire for this year's survey was focused on **six major areas** of consideration for adopting Cloud computing services from the SMEs' perspectives:

- IT security policy
- Physical security management
- Data privacy management
- System management
- Incident management
- Readiness on Privacy Protection

Security is still among their top consideration for SMEs when using or adopting the cloud services.

Compared against those who do not, **SMEs using Cloud services show a remarkably higher level of security readiness in their overall data management and information security systems, as well as in their ability to handle security incidents**. More than half of the SMEs who responded believed that they could rely on CSPs to provide them with the security required. This shows that data security should not be perceived as a barrier to using Cloud services; on the contrary, adopting Cloud services may be a solution to having and maintaining better overall information security.

Many SME owners already have some knowledge about security with Cloud services and its execution at the level of company policy. However, on a technical level, **a lot of companies are still lacking in awareness of the importance of having a security patch management policy,** which is a crucial element in protection a company's system.

On privacy and data protection issues, which has become one of SMEs major concern since the enactment of the Personal Data (Privacy) Ordinance PD(P)O, 45% of the SMEs do not want their CSPs to look at or use their data for marketing purpose but only 35% of them know whether the CSPs will use their data or not for such purpose. **A key success factor for popularization of Cloud Adoption would be for the CSPs to provide higher transparency to their security and privacy policy and measures for customers.**

With limited resources in manpower and specialized domain knowledge, SMEs should choose reliable and secure CSPs and commercial Cloud services with appropriate product features and business models to protect their company data and property more comprehensively and effectively. International standards like ISO/IEC 27017 and ISO/IEC 27018 can help in this regard. In identifying appropriate CSPs and Cloud services to use, customers can be assured that those CSPs that demonstrate compliance with ISO/IEC 27017 and ISO/IEC 27018 standard will have strong privacy and security protections in place. This will in turn facilitate compliance by the SMEs with their privacy obligations under the PD(P)O. SMEs can also follow the Security Guidance for Critical Areas of Focus in Cloud Computing and Cloud Controls Matrix (CCM released by CSA, and the Practical Guide for Procuring Cloud Services released by Office of the Government Chief Information Officer.

Organizers

Sponsor

Introduction and Background

This 2017 Hong Kong Small and Medium-sized Enterprises (SME) Cloud Adoption, Security and Privacy Readiness Survey was conducted by the Internet Society Hong Kong and the Cloud Security Alliance Hong Kong and Macau Chapter, who commissioned the Hong Kong Productivity Council (Council) to carry out telephone interviews with SMEs (<100 employees) in Hong Kong. The process was carried out over the course of three weeks and reviewed data from the Census and Statistics Bureau. The Council successfully collected 103 responses for the survey. The research covered major industry sectors in Hong Kong. The survey questionnaire was developed based on the Cloud Security Alliance Cloud Control Matrix and international standards with questions adapted to local conditions. The survey was sponsored by Microsoft Hong Kong.

Survey mechanism and technical information

The survey was conducted from March to April 2017 targeting SMEs in Hong Kong. Survey candidates were selected from HKPC's in-house database, industry directories, and the Hong Kong Yellow Pages.

Each SME was interviewed by telephone based on a structured Chinese questionnaire with 21 questions. A total of 103 questionnaires were completed at the end of the survey period. The 21 questions addressed the following areas of consideration for Cloud security:

- IT security policy
- Physical security management
- Data privacy management
- System management
- Incident management
- Readiness on Privacy Protection

Except for the first two questions about the background of the interviewees, interviewees were asked to answer the questions using a 1 to 5 scale indicating the SME's readiness in using Cloud services. A detailed analysis of the survey responses and our recommendations can be found in the following sections according to the respective areas of consideration.

Findings and recommendations

IT Security Policy

From the survey results, we can conclude that:

- 74% of companies surveyed have security policies in place (increased by 17%)
- 39% of companies surveyed perform security audit and certifications by external parties (decreased by 2.5%)
- 61% of companies surveyed have proper documentation on access rights management to data (increased by 17%)

Findings

We are seeing **an increase in the number of companies** (17% increase from last year's survey) **having formal security policies in place** for setting their information security blueprint. This shows companies are taking a more mature approach in planning and setting out formal information security plans and requirements.

We encountered an even **greater increase in the number of companies that hire external parties to conduct security audit and certification review**. Since we do not expect SMEs to possess in-house security audit personnel and have limited budget for information security, this significant increase suggests not only that are such audits and reviews becoming more common and affordable, but also that some business owners see that being recognized with proper certifications helps to build positive image and instill confidence in their customers.

In addition, the survey shows **an increase** (17%) **in respondents that have properly mapped out their data access rights management** to the various roles within the organization. This shows SMEs care about the data security.

Recommendations

While we see an increase in the number of SMEs having formal security policies and proper documentation on access rights management to data. Cost is probably still the largest barrier to hiring external auditors so selecting CSPs with formal security certifications and/or proof that independent third-party security audits have been performed on their infrastructure will help reduce the cost of such effort tremendously. In this way, the **SME can take advantage of Cloud services and reduce their overall IT costs, whilst still assuring themselves that concerns on security and access rights have been addressed**.

Physical Security Management

From the survey results, we can conclude that:

- 68% of the companies surveyed manage their IT systems with proper access rights and password control, as well as maintain appropriate audit trail and exercise. (increased by 15%)
- 51% of the companies surveyed have people or teams in charge of hardware / software maintenance, as well as support. (increased by 4%)

Findings:

Most companies (68% of respondents) manage their passwords, physical access rights, and IT assets properly. The percentage of companies adopting such controls has increased by 15% compared with last survey. From another perspective, there is over 30% of respondents have no or little proper physical control over their software and hardware access rights.

51% of respondents have designated personnel looking after hardware and software maintenance. This is some improvement (4% increase) compared with last survey. More than half of the SMEs are managing such tasks themselves. Nevertheless, having proper access rights management and password control still remains the responsibility of the SMEs. CSPs cannot decide for them the proper access rights to be assigned to each employee or customer for each of their data and services. Using default security settings provided by vendors and CSPs is risky and it is highly possible that these settings do not fit the specific requirements of the individual SMEs.

Recommendations:

Using a reliable CSP can help SMEs to save on cost and effort spent on physical security management. However, the SME will still remain responsible for managing access rights, and maintaining audit trails of software and hardware access. **We strongly recommend having a designated person to determine the access control matrix for employees and customers,** if access by customers is allowed. Most CSPs provide user-friendly interface for setting up such access rights and audit trials for each of the services the SME may subscribe to.

Data privacy management

From the survey results, we can conclude that:

- 74% of companies surveyed have good understanding of or have implemented data encryption; a big increase from last survey (increased by 32%)
- 62% of companies surveyed have a data disposal policy established, which compares favorably with last survey result (increased by 38%)

Findings:

Most companies seem to understand the need for having proper data access right management and backup, and nearly 75% of the companies surveyed have a good understanding or have implemented data encryption. Besides, companies understand now the importance of having a data disposal policy, over 60% of the surveyed companies this year with a big jump of 62% with last survey's result.

Recommendations:

Utilizing CSPs' services will allow SMEs to enjoy the benefits of protecting their data through enterprise-grade infrastructure, with an affordable investment. As more and more SMEs place their company data in the Cloud, it is important for them to **establish clear and concise data protection and disposal policies and ensure that the CSPs they engage have similar policies in place**.

System Management

From the survey results, we can conclude that:

- 30% of the companies surveyed implemented a security patches policy, and it is slightly better than last survey (increased by 7.5%).
- 68% of the companies surveyed installed firewall devices to further improve the security and it is slightly worse than last survey (decreased by 4%)

Findings:

Most companies surveyed are poor in implementing security patches in a timely fashion, even though most companies have implemented firewall protection solutions. One of the reasons may be that the companies now rely on external companies to perform security patching.

Recommendations:

All companies are reminded that they must keep security patches updated to mitigate security risks. Companies who use the Cloud services of a CSP that has a proper security patches policy in place can significantly reduce their risk of having outdated security patches in at least that part of their overall IT infrastructure. In this regard, **companies should review their vendors' (and/or CSPs') solutions and security patches policies cautiously**. Companies can refer to the Threat & Vulnerability Management, as well as the Infrastructure & Virtualization Security sections of the CSA Cloud Control Matrix V3.0 to adopt the best practices.

Incident management

From the survey results, we can conclude that:

- 71% of the companies surveyed have established an Incident Response Plan and it's better than last year's result (increased by 39%)
- 73% of the companies surveyed also have a Disaster Recovery Plan in place and this is better than last year's result as well (increased by 25%)

Findings:

71% of the companies have an incident response and disaster recovery plan in place. The big jump in the number of companies that have such plans in place, as compared to the previous survey result, could be due to SMEs care about business continuity. However, for the companies claimed to have such measures in place, the maturity and effectiveness of their plans are questionable.

Recommendations:

The use of Cloud services can help companies with their incident response and disaster recovery, as most CSPs will have in-built incident response disaster recovery mechanisms in place. Nonetheless, companies will still need to have and maintain their own incident response and disaster recovery plans to meet their unique business and customer requirements, and which factors in the role of CSPs in incident response and disaster recovery. **Companies will also need to keep their incident response and disaster recovery plans up-to-date, and conduct regular drills to make sure the plans can perform as designed.** Again, SMEs can leverage on CSA's Security Guidance for Critical Areas of Focus in Cloud Computing and Cloud Controls Matrix (CCM) for information.

Understand SMEs readiness on privacy protection when using Cloud services

From the survey results, we can conclude that:

- For those companies who use Cloud services:
  - 95% follow the guidance from Office of the Privacy Commissioner for Personal Data (PCPD) to protect personal data, it is better than last survey. (increased by 38%).
  - 45% disagree that their CSPs look at and use their company or customer data for marketing purpose, it is not as well as last survey. (decreased by 12%)
  - 20% do not know if their CSPs will look at and use their company or customer data for marketing purpose, it is better than last survey of 26%.
  - 30% use CSPs who do not have transparency to their users on if and when their company or customer data will be deleted or returned. It is not as well as last survey of 49%.
  - 15% do not know if and when their CSPs will return or delete their company or customer data, it is better than last survey of 25%.
  - 45% use CSPs who do not have transparency to their users on which subcontractor they are employing to handle their company or customer data, it is not as good as last survey of 39%
  - 20% do not know if their CSPs have transparency to their users on which subcontractor they are employing to handle their company or customer data, it is better than last survey of 32%.
  - 25% use CSPs who do not/likely do not comply with guidance from PCPD to protect personal data, it is better than last survey of 30%.
  - 5% do not know if their CSPs will comply with guidance from PCPD to protect personal data, it is better than last survey of 18%.
  - 70% use CSPs who do not/likely do not understand or come across the cloud security standards such as ISO/IEC 27017 or MTCS SS[1].
  - 70% use CSPs who do/likely do agree the security standard is an important factor.
  - For those companies who do not use Cloud services, 69% do not understand or care the cloud security standards but over 50% agree the security standard is an important fact.

[1] Multi-Tier Cloud Security (MTCS) Singapore Standard https://www.imda.gov.sg/industry-development/infrastructure/ict-standards-and-frameworks/mtcs-certification-scheme

Findings:

While most of the companies (95%) claimed they follow the PD(P)O (Ordinance) from PCPD, one fifth of them (20%) do not know if their CSPs will use their data for marketing purposes. Besides, a considerable portion of companies (30%) use CSPs who do not have transparency to their users on which subcontractor they are employing to handle the data. Similarly some of the companies (25%) use CSPs who do not/ likely do not follow the Ordinance and this raises a significant concern as CSPs are also data processors of the companies. The companies will still be held accountable if there is any personal data breach by their CSPs.

In addition, nearly half of the companies (45%) use CSPs who do not have transparency to their users if and when their data can be deleted and returned. They might face difficulty when they want to unsubscribe from the Cloud services as the CSPs might not be able to return or securely delete their data.

Recommendations:

More education is needed to raise awareness among SMEs of the need to understand the CSPs' service terms on data privacy protection before signing up to the CSPs' Cloud services. Such awareness is especially important for SMEs intending to use the Cloud services of CSPs that rely on the use of customer data for other purposes (e.g. ad delivery and/or marketing) to support their business model and provide free services. For SMEs who are using Cloud service already, they are encouraged to revisit the service terms of the CSPs to avoid misunderstanding, in particular the terms related to the use of their data for other purposes.

To avoid vendor lock-in, **SMEs should be clear on the CSPs' policies for data retention and deletion**, including for when the SMEs unsubscribe from the Cloud services in question. This is also important to support the implementation of SMEs' **own data disposal policy** vis-à-vis the SME's customers. (Please refer to Data Privacy Management)

Moreover, it is sometimes hard for SMEs to know which CSPs follow the Ordinance or similar international legislations to protect their personal data. It is recommended that **SMEs should look for CSPs who comply with international standards like ISO/IEC 27017 and ISO/IEC 27018** which provides guidelines for CSPs concerning the protection of Personally Identifiable Information.

Conclusion

While security remained SMEs' a major concern in using Cloud services, more than half of the SMEs believed that they can rely on the CSPs to provide the security for them.

The other major concern for SMEs when using Cloud services is data privacy. After the enactment of the PC(P)O, 95% of the SMEs have policies to comply the Ordinance. However, a quarter of the SMEs surveyed are not sure how their CSPs would use their data. Hence, when SMEs choose their CSPs, they need to ensure their CSPs can help them protect data privacy and personal data from both technical features and the business model perspectives. Where SMEs do not have the sufficient expertise to ascertain which CSPs can protect the

privacy of their data, reliance on international standards, such as ISO/IEC 27018, can help such SMEs choose appropriate CSPs.

The results of this Cloud Adoption, Security and Privacy Readiness Survey give a positive outlook for Cloud technology. Most of the respondents have indicated they are aware of the security requirements of adopting such technology, and many of such SMEs are already using many types and/or the subsets of Cloud services. But as we all know in the practical world, technology is always on the move and more can be done to raise awareness among SMEs of the benefits of Cloud services to allow such services to be more easily and confidently adopted by SMEs, especially considering that such businesses would benefit most from the use of such services.

Organizers

Sponsor

About the Cloud Security Alliance Hong Kong and Macau Chapter
The Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing. CSA is led by a broad coalition of industry practitioners, corporations, associations and other key stakeholders. The CSA Hong Kong and Macau Chapter was launched in 2012 by a group of local IT professionals, to further expand its presence and focus in Asia-Pacific,

About the Internet Society Hong Kong
Internet Society Hong Kong (ISOC HK) is the local chapter organization of the Internet Society (ISOC), which is an international and not-for-profit membership society. ISOC HK was formed in 2005 by local veteran Internet professionals with the mission to improve the practice of Internet governance and online civil society in Hong Kong. Consistent with the ISOC statement of purpose, ISOC HK believes in “maintaining and extending the development and availability of the Internet and its associated technologies and applications – both as an end in itself, and as a means of enabling organizations, professions, and individuals locally and worldwide to more effectively collaborate, cooperate, and innovate in their respective fields and interests.”

About Microsoft
Founded in 1975, Microsoft (Nasdaq “MSFT”) is the worldwide leader in software, services and solutions that help people and businesses realize their full potential.

Appendix I – Survey Questionnaire

APPENDIX I (FINAL VERSION)

香港中小企雲端應用, 保安及私隱就緒程度調查 2017 – 問卷
Hong Kong SME Cloud Security & Privacy Readiness Survey 2017– Questionnaire

調查簡介
您好！香港互聯網協會及香港生產力促進局正進行一項有關雲端應用及保安就緒程度的調查。現誠邀 閣下參與。是次調查可於 10 分鐘內完成。

A. 公司資料確認

Q-1. 貴公司現時於香港辦公室之總員工人數：_____ (Q1)
(註：中小企業 = 於香港聘用 10–100 名員工；如受訪公司未能符合上述定義，需終止訪問)

Q-2. 貴公司主要業務為：*(只可單選)* (Q2)

1. □製造
2. □進出口貿易及批發
3. □零售 4. □住宿及膳食服務 5. □資訊及通訊 6. □金融及保險
7. □專業服務(包括法律、會計、顧問服務、廣告、室內設計) 8. □地產(包括地產經紀、裝修)
9. □醫療(包括醫療服務、設備及藥物) 10. □運輸物流(包括客運、貨運、貨倉、速遞) 11. □互聯網(網上服務、程式開發)

12.□其他(請註明)：_____

於以下部份，請就有關句子，於 4 個答案選項中，選出最符合 貴公司現時情況的一個選項。

B. 公司整體資訊保安政策（IT Security Policy)

句子	答案選項	完全不符合(1)	少部份符合(2)	大部份符合(3)	完全符合(4)
Q-3. 公司具備正式的資訊保安措施，以監察、審核及持續提升全公司的資訊保安水平。	(5) = 不確定				
Q-4. 公司的資訊保安措施，每年均會由外間獨立機構／人士透過審計（Auditing）或再續証（Certification）等過程，進行檢視。	(5) = 不確定				
Q-5. 公司具備守則文件，闡述不同崗位員工的資訊存取權限，並指示如何處理離職或內部轉職員工之資訊存取權，包括刪除及更改存取權。	(5) = 不確定				

C. 實體保安管理（Physical Security Management）

句子	答案選項	完全不符合(1)	少部份符合(2)	大部份符合(3)	完全符合(4)
Q-6. 公司透過一系列措施，包括為不同崗位員工制定使用權限、採用密碼、保存使用記錄或進行審計等，以便中央管理公司的資訊科技系統（如伺服器）。	(5) = 不確定				
Q-7. 公司有專責職員管理內部資訊科技資產，包括中央監察相關軟硬件的保養期，及中央統籌相關軟硬件的支援。	(5) = 不確定				

D. 數據保安管理（Data Privacy Management）

句子	答案選項	完全不符合 (1)	少部份符合 (2)	大部份符合 (3)	完全符合(4)
Q-8. 公司有採用數據加密技術於資訊系統上，以加強保護內部資料數據，防止外洩，並定期檢視數據保安情況。	(5) = 不確定				
Q-9. 公司具備守則文件以指示員工銷毀內部數據，並會保留數據銷毀紀錄，以及定期檢討數據銷毀過程。	(5) = 不確定				

E. 系統管理（System Management）

句子	答案選項	完全不符合 (1)	少部份符合 (2)	大部份符合 (3)	完全符合(4)
Q-10. 內部專責職員通常於修補程式（Patch）發佈後的一段固定時間內（如發佈後一個月內），測試修補程式。通過測試後，修補程式會被自動安裝於公司所有連接網絡的電腦內。	(5) = 不確定				
Q-11. 除了使用互聯網服務供應商的防火牆外，公司亦自行裝設額外防火牆（硬件或軟件）以加強保護。公司會中央管理該防火牆，並會定期為該防火牆進行審計工作。	(5) = 不確定				

F. 事故處理（Incident Management）

句子	答案選項	完全不符合 (1)	少部份符合 (2)	大部份符合 (3)	完全符合(4)
Q-12. 公司具備守則文件以指示員工處理內部資訊保安事故（例如電腦失竊、資料外洩）。公司亦會定期檢視、測試及更新相關守則。	(5) = 不確定				
Q-13. 公司備有災難復原計劃（Disaster Recovery Plan）、備用電腦和備份數據庫，以便於資訊保安事故後，盡快恢復公司運作。公司亦定期檢視和測試災難復原計劃。	(5) = 不確定				

G. 雲端資訊科技應用情況（Cloud Technology Application）

Q-14. 貴公司有否使用任何雲端資訊科技應用方案？（「雲端資訊科技應用」定義：讓中小企透過互聯網和流動網絡，以相對低廉的起動成本，採用切合其運作規模的資訊科技應用 – 出自立法會）

1. □ 現正使用 [至 Q15]
2. □ 現在沒有使用，但正考慮／研究相關方案 [至 Q18]
3. □ 現在沒有使用，短期內亦不考慮 [至 Q18]

[Q14 答 - 現正使用]

Q-15. 哪類型的雲端資訊科技應用方案?請註明（可選多項）：

1. □電郵 2. □辦公室協作工具 3. □銷售 4. □客戶關係管理 5. □資料存儲 6. □雲端保安
7. □財務 8. □企業資源規劃 9. □人力資源管理 10. □數據運算 11. □軟件開發 12. □軟件測試
13. □其他（請註明）：_____

Q-16. 於以下部份，請就有關句子，於 4 個答案選項中，選出最符合貴公司現時情況的一個選項。

句子	答案選項 完全不符合(1)	少部份符合(2)	大部份符合(3)	完全符合(4)
(a) 你的公司已經遵循本地私隱專員的指引，以保護個人資料？	(5) = 不確定 / 沒有意見			
(b) 你已經同意雲端服務供應商可以查看和使用您公司或客戶的信息於廣告或促銷的用途？	(5) = 不確定/ 沒有意見			
(c) 你的雲端服務供應商已經提供明確的時間表於何時退回或刪除您公司或客戶的信息？	(5) = 不確定/ 沒有意見			
(d) 你的雲端服務供應商已經透明地提供有可能將處理您的公司或客戶信息的外判商身份？	(5) = 不確定/ 沒有意見			
(e) 你的雲端服務供應商已經遵循本地私隱專員的指引，以保護個人資料？	(5) = 不確定/ 沒有意見			
(f) 你認識／聽過雲端相關保安標準（如 ISO27017／MTCS SS）	5) = 不確定/ 沒有意見			
(g) 保安標準是你選擇雲端服務供應商的重要因素	5) = 不確定/ 沒有意見			

Q-17. 請闡述使用雲端資訊科技應用方案的原因（可選多項）：

1. □起首的投資較少（軟／硬件） 2. □費用投資方面的彈性較大 3. □可倚賴方案供應商的支援
4. □可倚賴方案供應商的資訊保安功能 5. □雲端服務的系統比較自己的系統穩定
6. □可享用最新功能或科技 7. □其他（請註明）：

_____

Q-18. 如果根據以下 4 個主要雲端服務供應商，你會優先考慮使用哪一間的服務？請排序 **(1 為最先考慮)**

a) 1._____, 2._____, 3._____, 4._____

i)Amazon Web Services ii)Microsoft Azure iii)IBM iv)VMware

[不主動提出選項] 5. □ 選擇其他供應商，例如(i)_____

b) 優先考慮的主要因素

1. □品牌信譽 2. □有使用該公司其他解決方案 3. □價錢4. □服務內容
5. □其他（請註明）：_____

[完成問卷]

[Q14 答-現在沒有使用]

Q-19. 於以下部份，請就有關句子，於 4 個答案選項中，選出最符合 貴公司現時情況的一個選項。

句子	答案選項	完全不符合(1)	少部份符合(2)	大部份符合(3)	完全符合(4)
(h) 你的公司已經遵循本地私隱專員的指引，以保護個人資料？		(5) = 不確定 / 沒有意見			
(i) 你會同意雲端服務供應商可以查看和使用您公司或客戶的信息於廣告或促銷的用途？		(5) = 不確定 / 沒有意見			
(j) 你會要求你的雲端服務供應商提供明確的時間表於何時退回或刪除您公司或客戶的信息？		(5) = 不確定 / 沒有意見			
(k) 你會要求你的雲端服務供應商透明地提供有可能將處理您的公司或客戶信息的外判商身份？		(5) = 不確定 / 沒有意見			
(l) 你會要求你的雲端服務供應商遵循本地私隱專員的指引，以保護個人資料？		(5) = 不確定 / 沒有意見			
(m) 你認識／聽過任何雲端相關保安標準（如 ISO27017／MTCS SS）		(5) = 不確定 / 沒有意見			
(n) 保安標準是你選擇雲端服務供應商的重要因素		(5) = 不確定 / 沒有意見			

Q-20. 請闡述不使用雲端資訊科技應用方案的原因（可選多項）：

1. □對雲端資訊科技認識不深
2. □資訊保安的考慮
3. □感覺上，雲端服務不太穩定
4. □害怕雲端服務供應商倒閉，因而損失正使用的雲端方案中的數據
5. □害怕雲端服務供應商倒閉，因而損失所繳費用
6. □害怕雲端服務供應商查看或使用您公司或客戶的信息於其他用途
7. □害怕不符合法規/合規要求
8. □其他（請註明）：_____

Q-21. 如果根據以下 4 個主要雲端服務供應商，你會優先考慮使用哪一間的服務？請排序(1 為最先考慮)

a) 1._____, 2._____, 3._____, 4._____

i)Amazon Web Services ii)Microsoft Azure iii)IBM iv)VMware

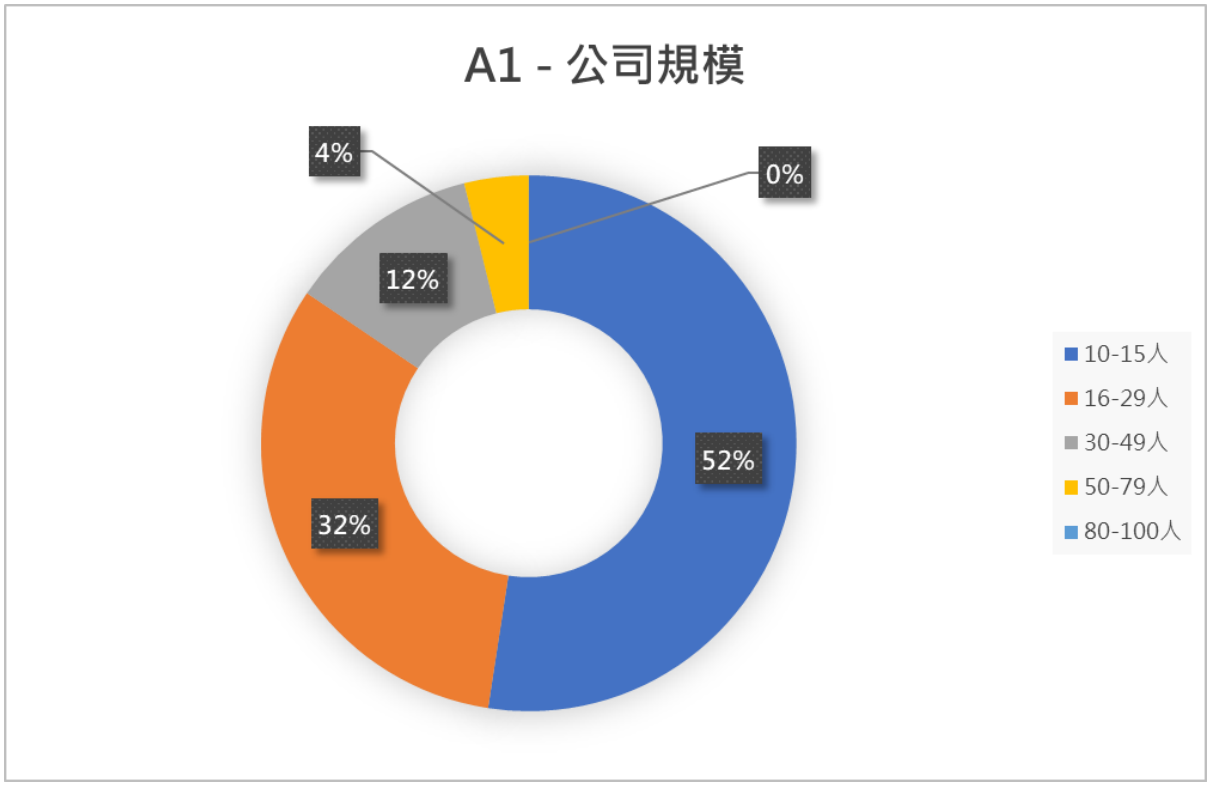
[不主動提出選項] 5. □ 選擇其他供應商，例如(i)_____

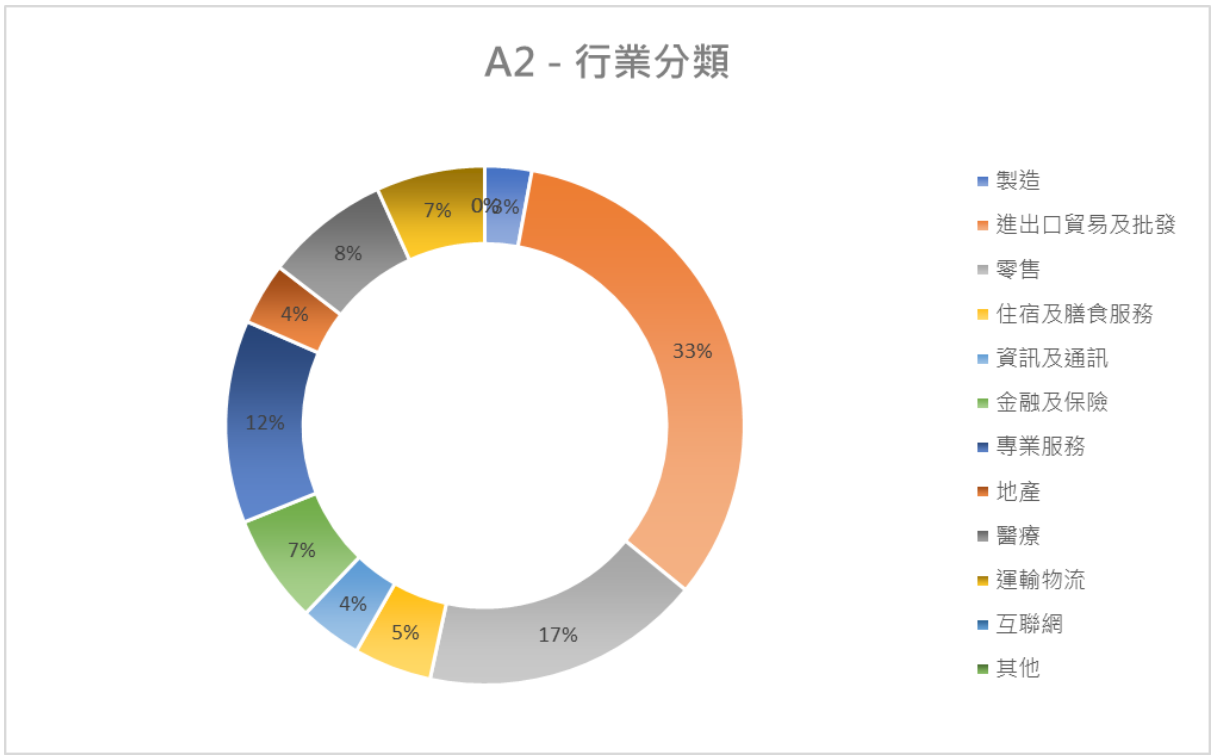
b) 優先考慮的主要因素

1. □品牌信譽 2. □有使用該公司其他解決方案 3. □價錢 4. □服務內容
5. □其他（請註明）：_____

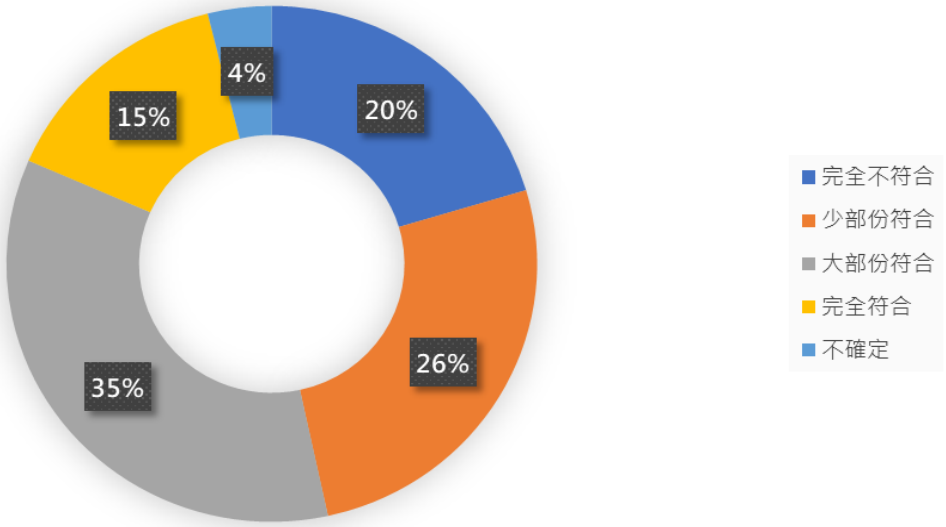
問卷完

Appendix II - Statistics and Charts

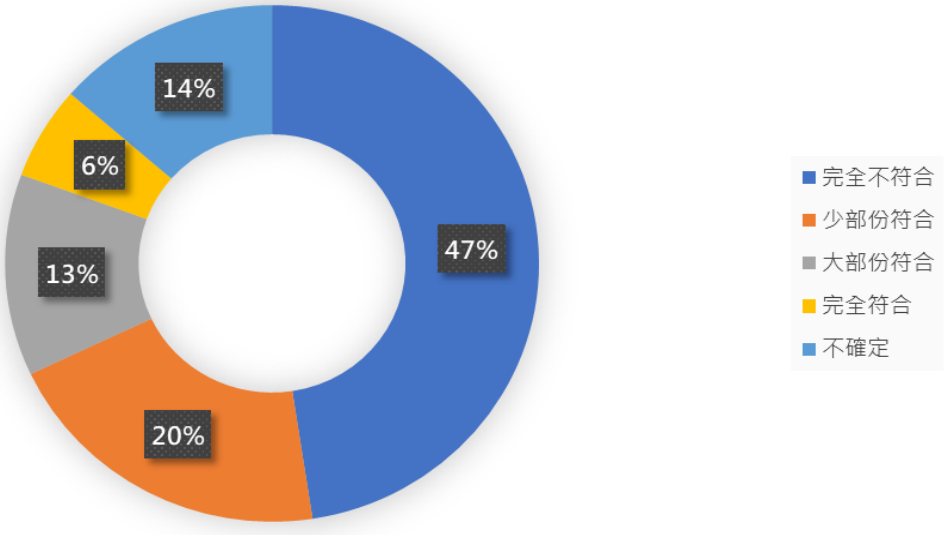




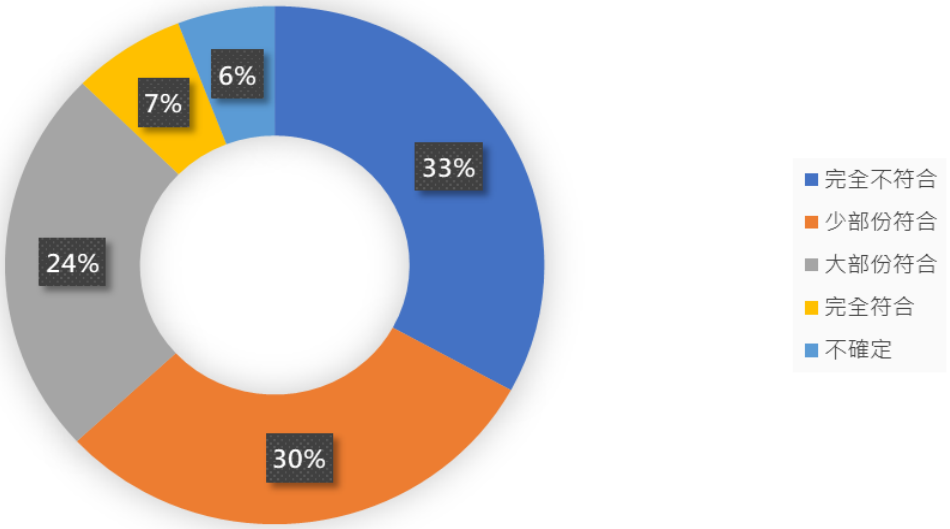
B3 - 具備正式資訊保安措施



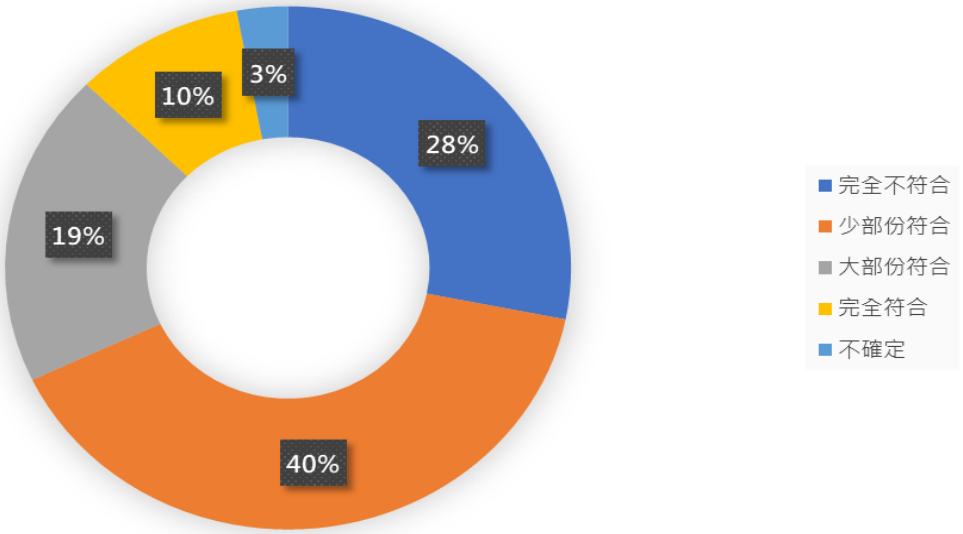
B4 - 每年由外間機構檢視資訊保安措施



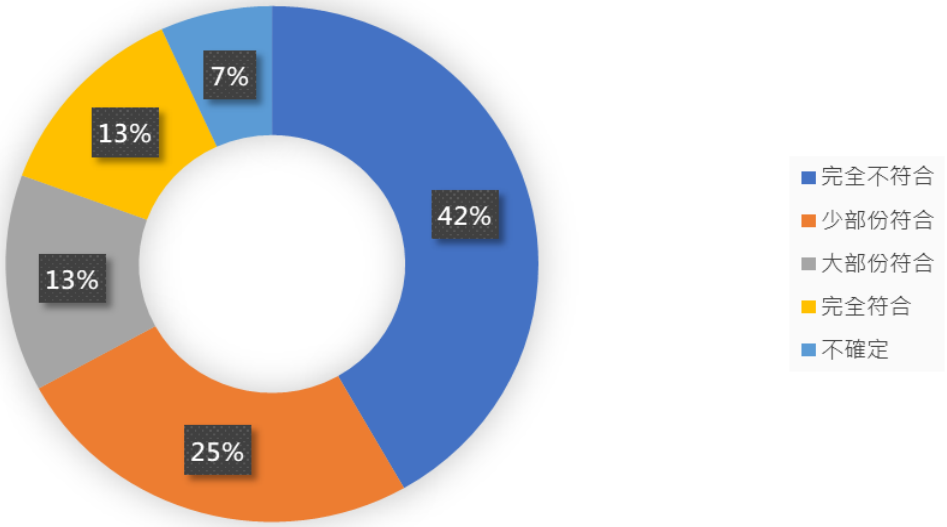
B5 - 具備正式資訊存取權限之守則



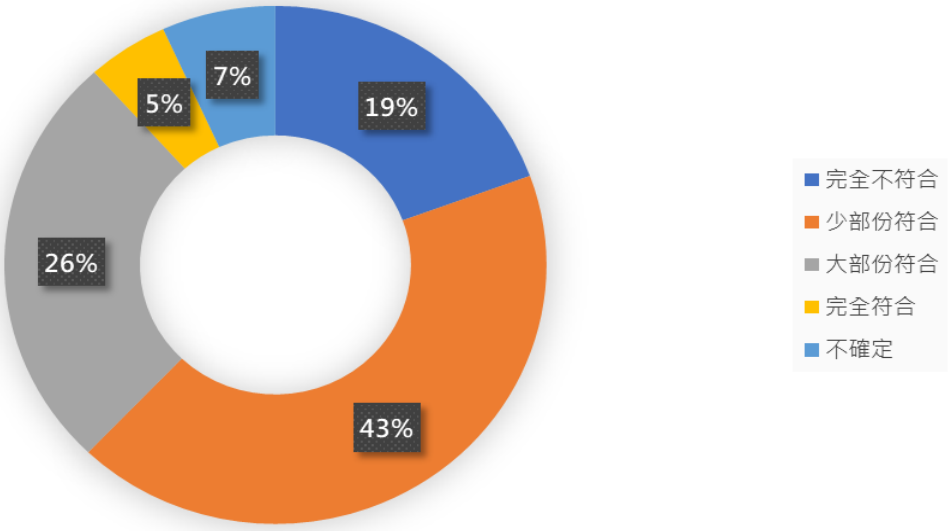
C6 - 公司透過中央管理資訊系統保安



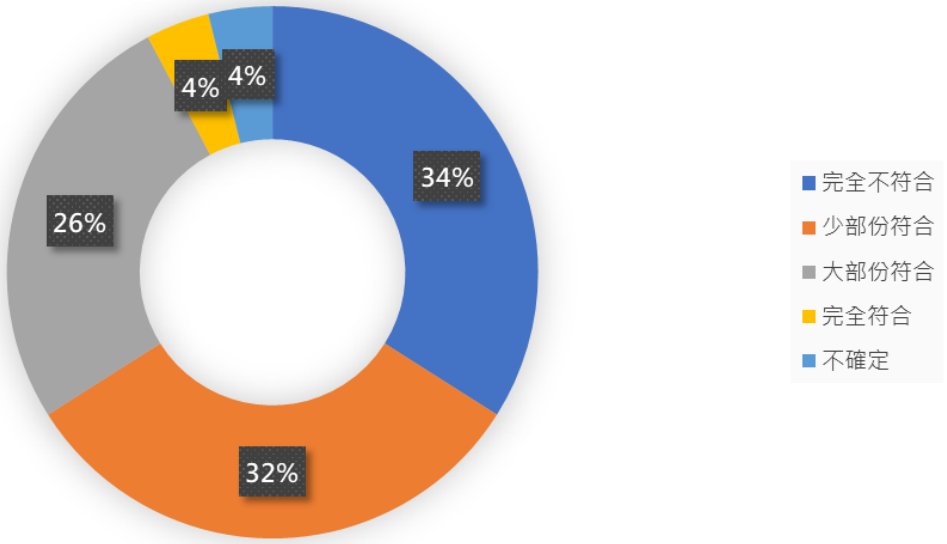
C7 - 設有專人管理資訊系統



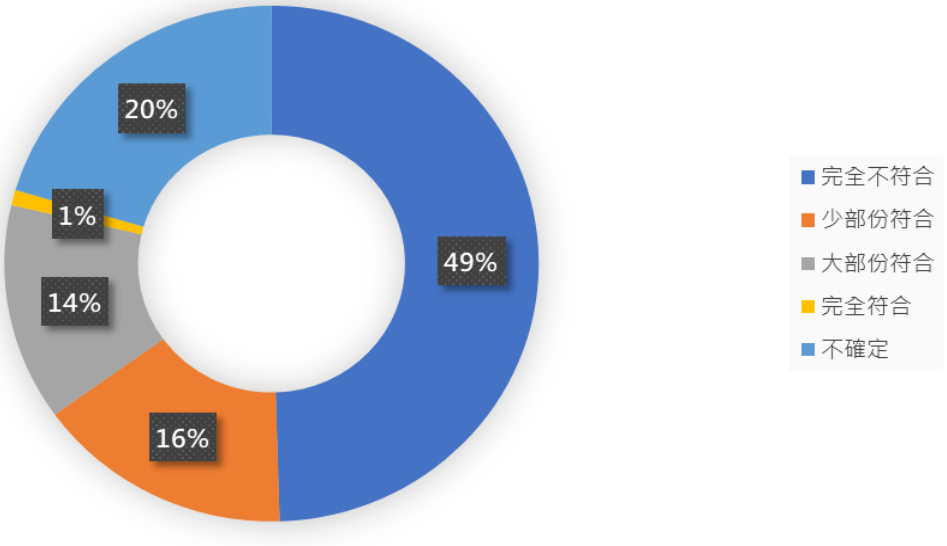
D8 - 公司有使用到加密技術保護資料



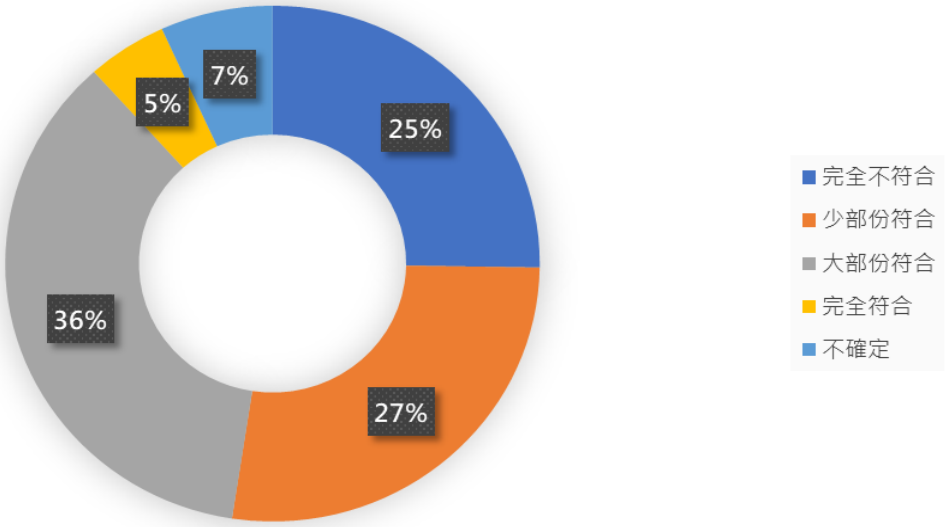
D9 - 公司設有數據銷毀的程序



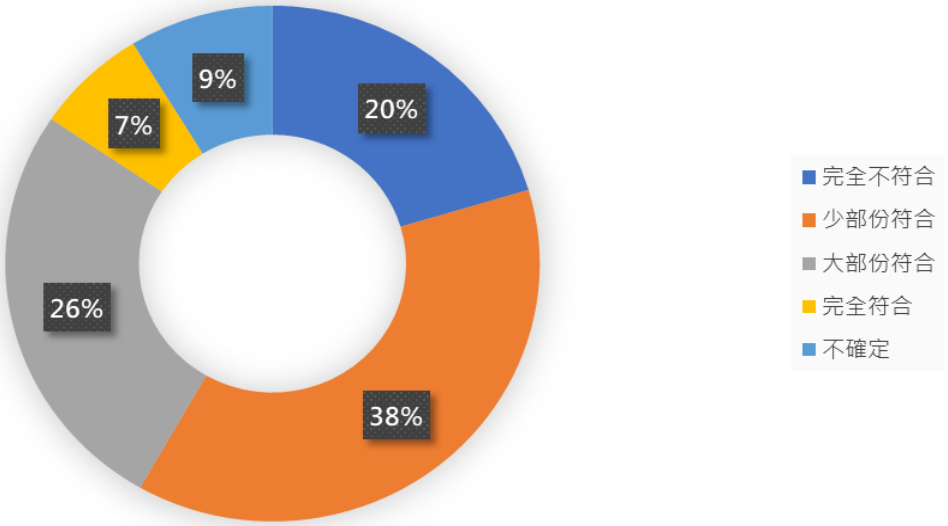
E10 - 設有專人管理修補程式

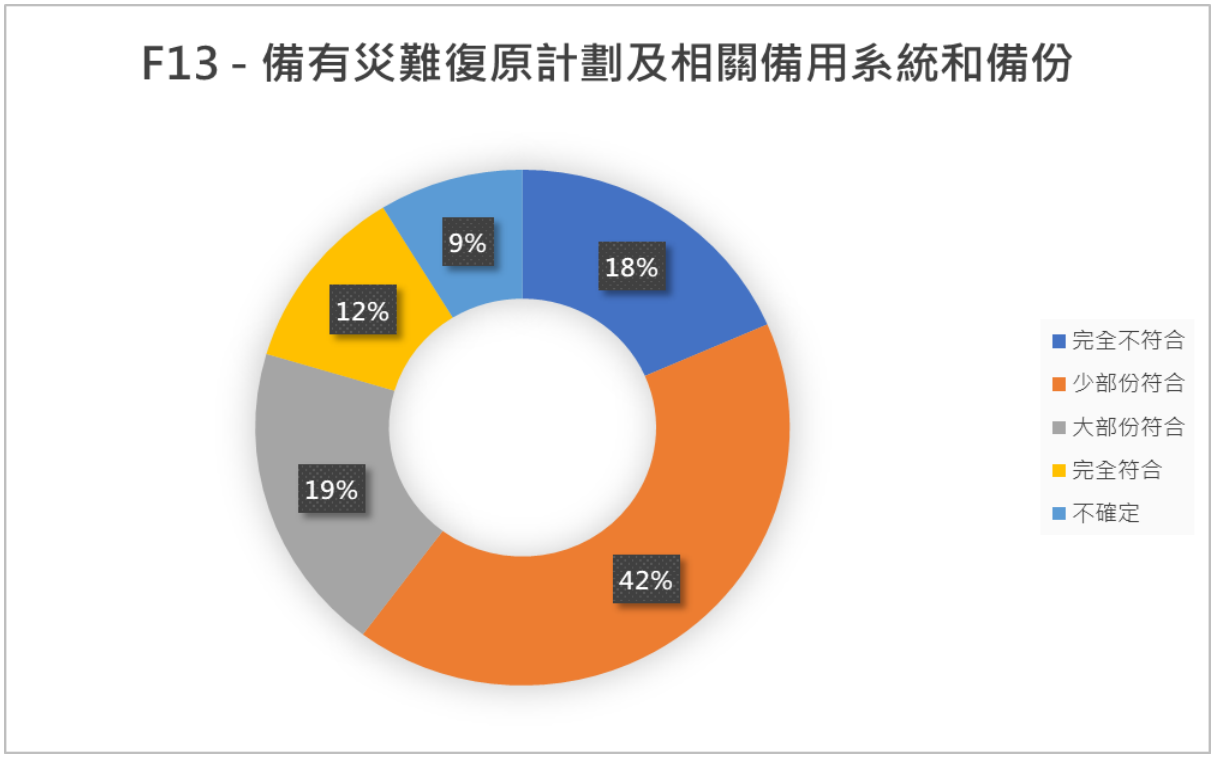


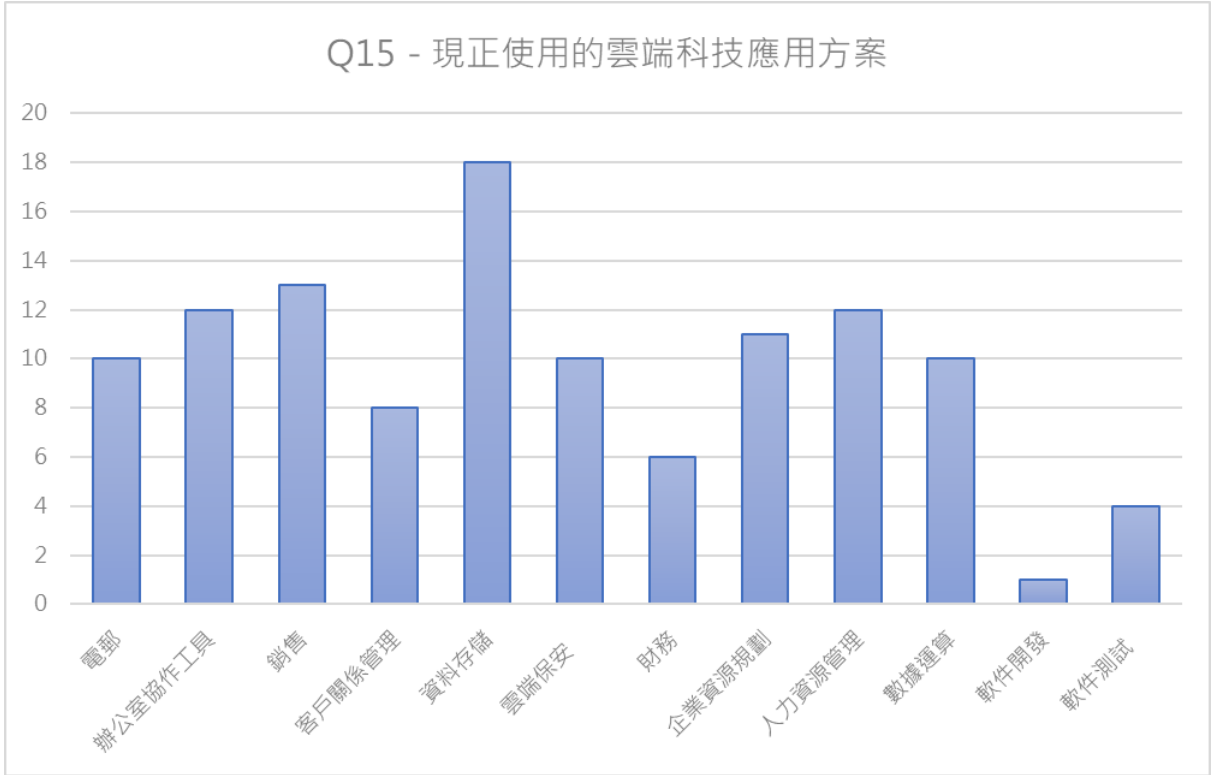
E11 - 自行設置及管理防火牆



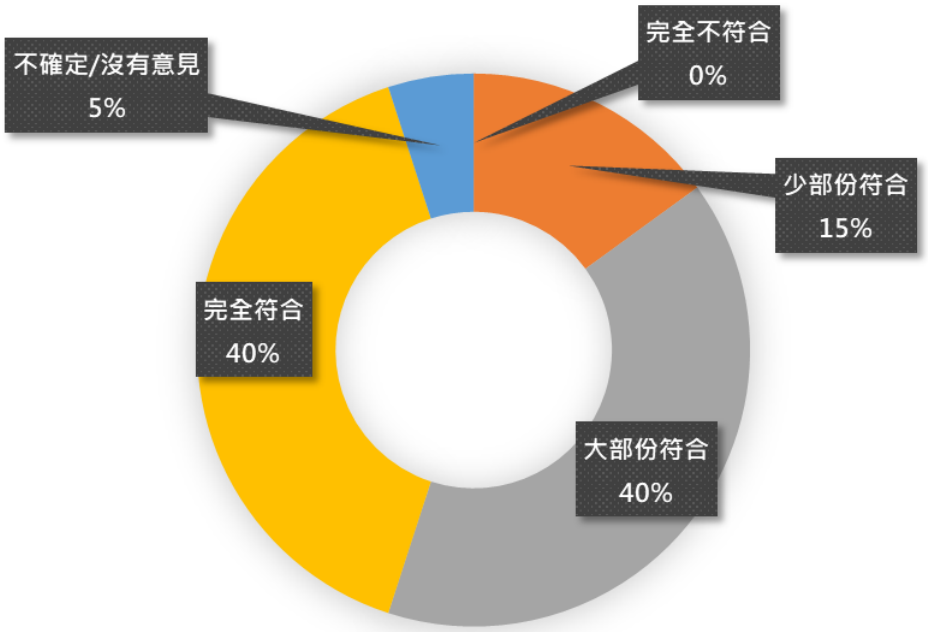
F12 - 設有守則處理資訊保安事故



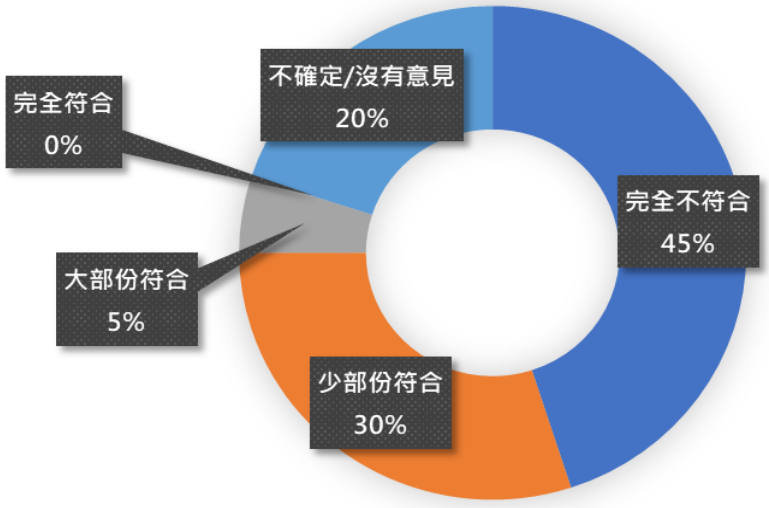

F13 - 備有災難復原計劃及相關備用系統和備份
18%
42%
19%
12%
9%
完全不符合
少部份符合
大部份符合
完全符合
不確定


Q15 - 現正使用的雲端科技應用方案
20
18
16
14
12
10
8
6
4
2
0
電郵
辦公室協作工具
銷售
客戶關係管理
資料存儲
雲端保安
財務
企業資源規劃
人力資源管理
數據運算
軟件開發
軟件測試

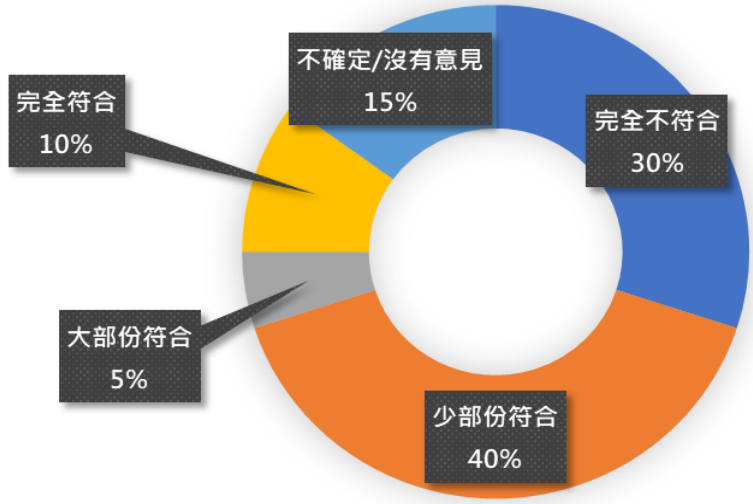
G16a - 你的公司已經遵循本地私隱專員的指引，以保護個人資料



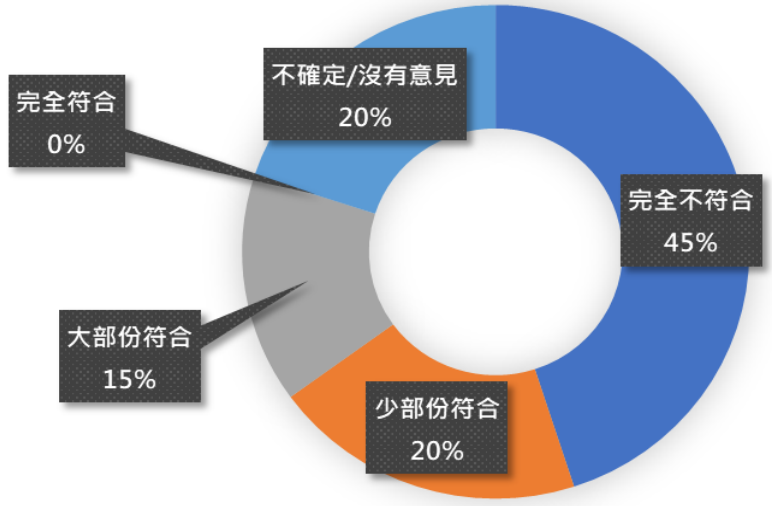
G16b - 你已經同意雲端服務供應商可以查看和使用您公司或客戶的信息於廣告或促銷的用途



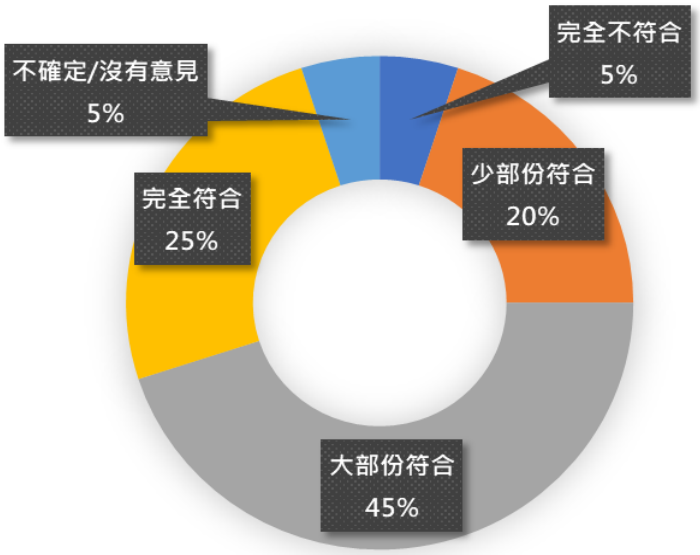
G16c - 你的雲端服務供應商已經提供明確的時間表於何時退回或刪除您公司或客戶的信息



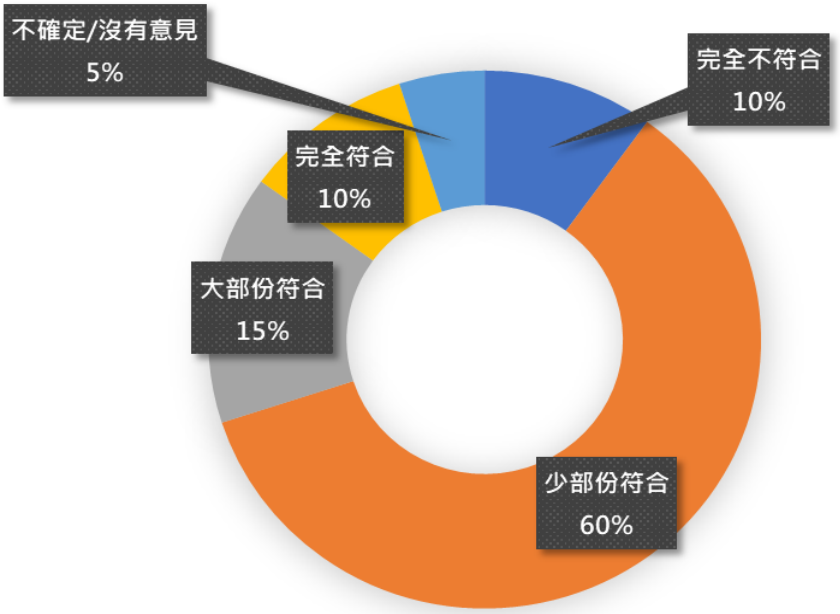
G16d - 你的雲端服務供應商已經透明地提供有可能將處理您的公司或客戶信息的外判商身份

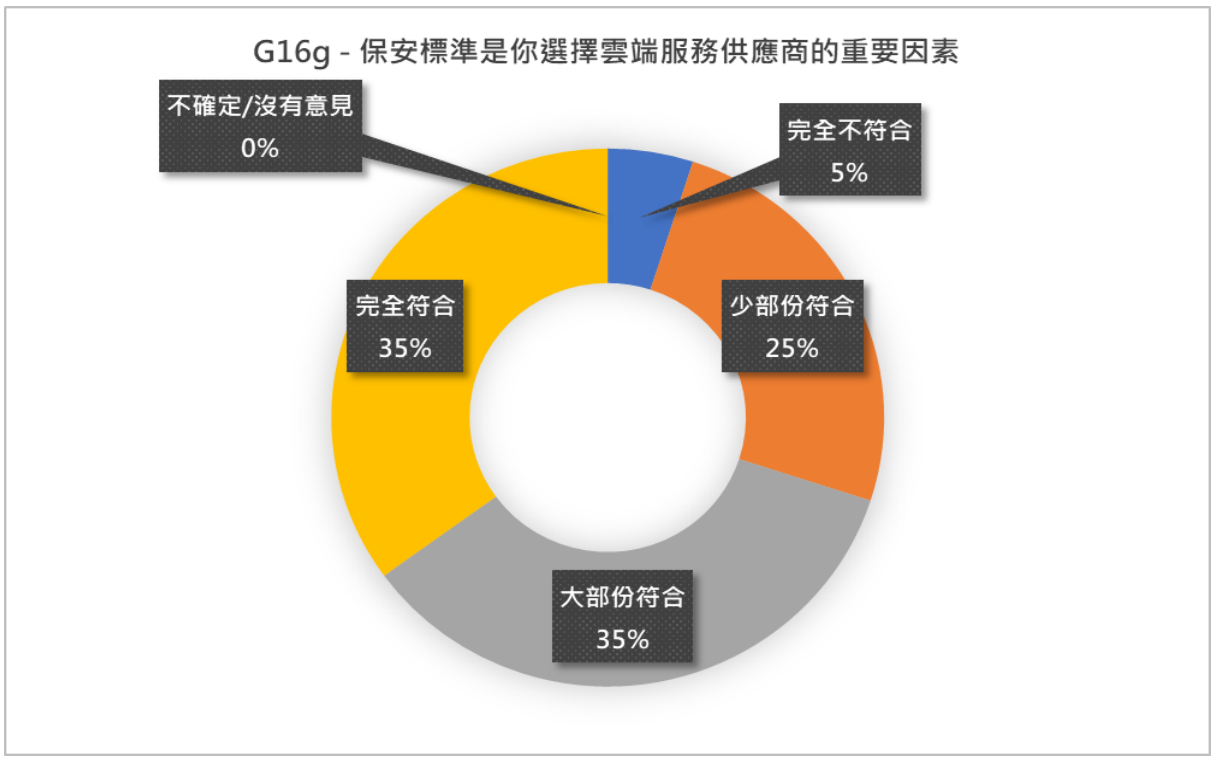


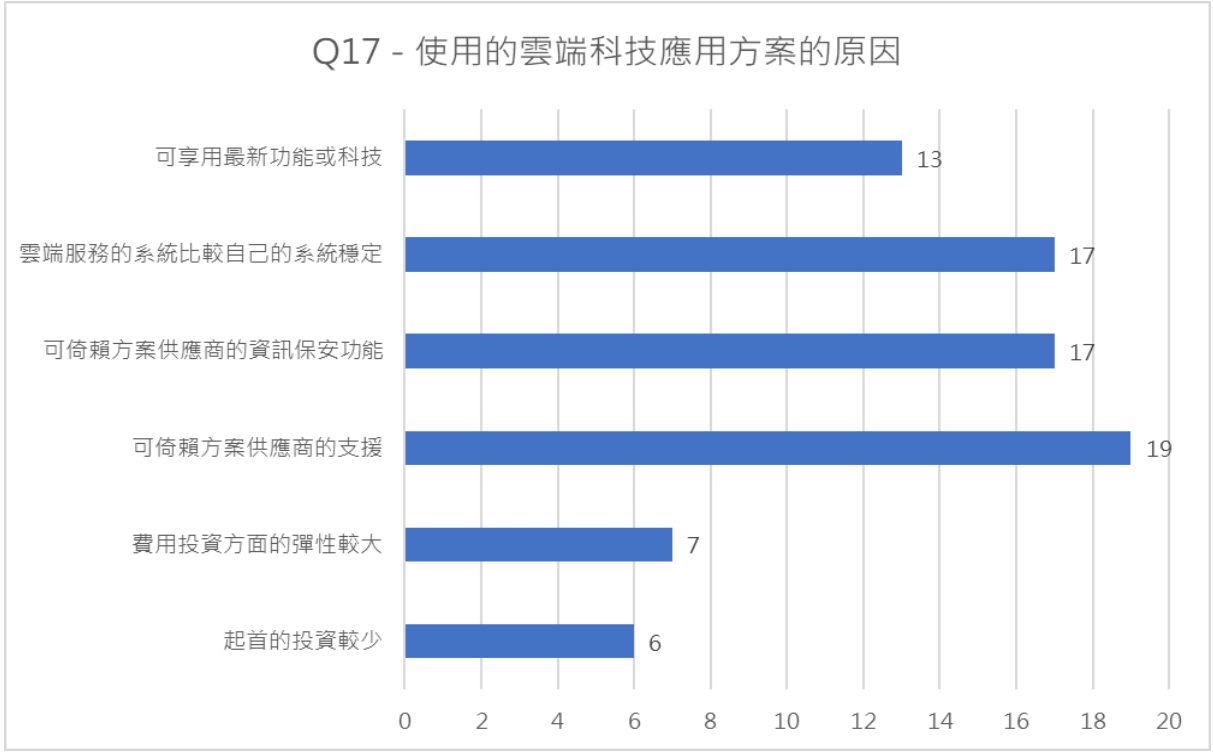
G16e - 你的雲端服務供應商已經遵循本地私隱專員的指引，以保護個人資料



G16f - 你認識 / 聽過雲端相關保安標準

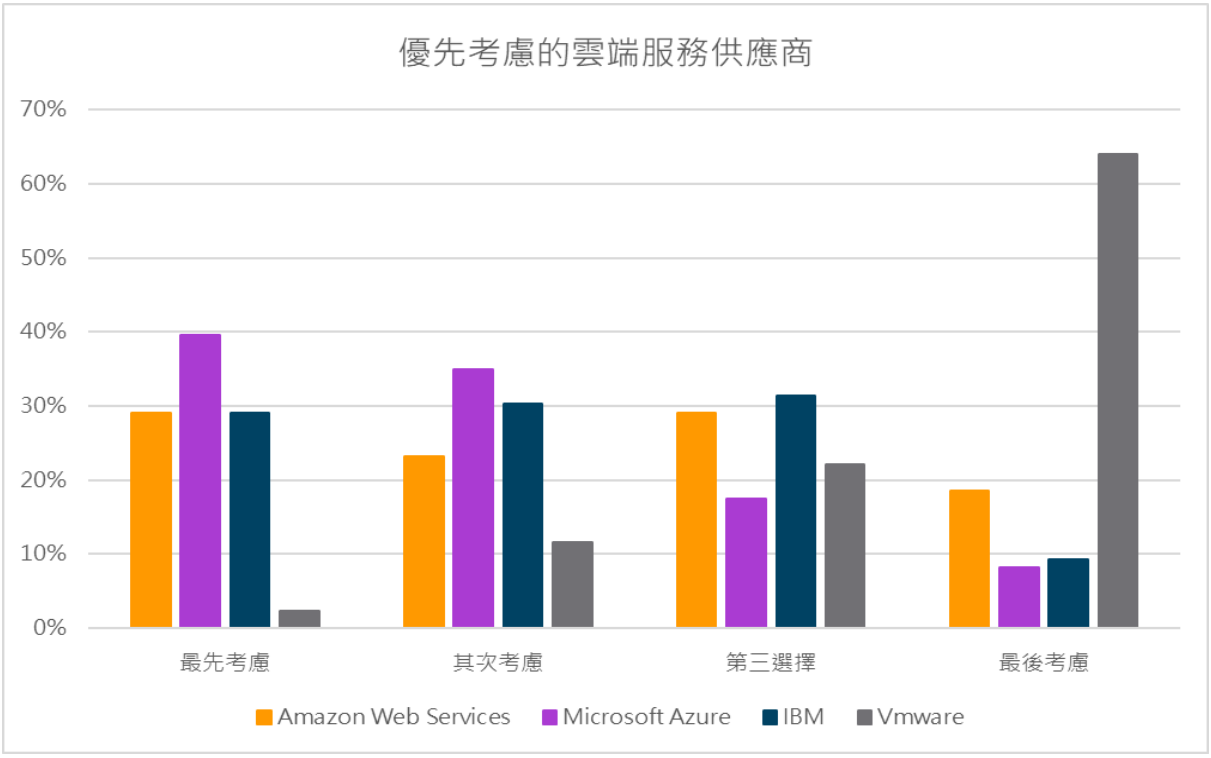



G16g - 保安標準是你選擇雲端服務供應商的重要因素
不確定/沒有意見
0%
完全不符合
5%
完全符合
35%
少部份符合
25%
大部份符合
35%


Q17 - 使用的雲端科技應用方案的原因
可享用最新功能或科技
13
雲端服務的系統比較自己的系統穩定
17
可倚賴方案供應商的資訊保安功能
17
可倚賴方案供應商的支援
19
費用投資方面的彈性較大
7
起首的投資較少
6
0
2
4
6
8
10
12
14
16
18
20

Organizers

Sponsor



Appendix III – ISO/IEC 27018 background information

The new standard, ISO/IEC 27018 (ISO 27018), strengthens data privacy by adding key protections for sensitive customer information stored in the Cloud. Published July 30th, 2014 by the International Organization for Standardization (ISO), it sets forth guidelines for Cloud service providers concerning Personally Identifiable Information ("PII"). The standard was developed in consultation with contributors from 14 countries and 5 international organizations.

Modernizing security and privacy in the Cloud

Before ISO/IEC 27018, there wasn't a robust, internationally-recognized benchmark for protecting Cloud stored PII. The well-established ISO/IEC 27001:2013 international standard provides a flexible system for identifying information security risks and choosing controls to address them. As an addendum to ISO/IEC 27001, ISO/IEC 27018 provides specific guidance to Cloud Service Providers (CSP) for assessment of risks and implementation of state-of-the-art controls for protection of PII stored in the Cloud.

Why does an international standard matter?

It is critical that new guidance and controls for PII be defined in international standards. International standards provide at least three key characteristics.

- **Trust.** International standards are created according to strict rules that ensure multiple stakeholders participate in an extensive review process.
- **Acceptance.** International standards from ISO are accepted by all but a few governments as a basis for policy, procurement and trade rules.
- **Global reach**. The global acceptance of ISO standards supports cross-nation business and trade.

Why does adopting ISO 27018 controls matter?

- A Cloud service's audited compliance with the controls in ISO/IEC 27018 gives customers **an easy way to confirm that the personal information they entrust to the CSP will be used only as they approve and is kept secure.** This is particularly important for government customers, who are often subject to stricter obligations to protect information in their care.
- The ISO/IEC 27018 standard supports regulations set by data protection authorities around the world. Since the standard incorporates the input of multiple regional regulators, use of Cloud services that comply with it **demonstrates support for the requirements of many local Data Protection Authorities.** This standard **brings a welcome degree of uniformity to the industry, and adds needed protections to improve PII security and compliance** in an increasingly Cloud-based information environment.

- ISO/IEC 27018 gives new, clear guidance based on EU Data Protection Authorities input on **how a data processor should protect customer data**, including a requirement that providers must either not mine customer data for advertising purposes, or gain explicit consent to do so. Moreover, it must be possible for a customer to use the service without submitting to such use of personal data for advertising or marketing.

- ISO/IEC 27018 **helps customers and CSPs by ensuring that concrete guidance and specific controls for processing PII are addressed** as part of an ISO/IEC 27001 audit. Adding the guidance and controls of ISO/IEC 27018 to third-party audits provides evidence of that commitment.

Cloud service providers adopting ISO/IEC 27018 must operate under six key principles:

1. **Consent**: CSPs must not process the personal data they receive for purposes independent of the instructions of the customer, and they must not use that personal data for advertising and marketing unless expressly instructed to do so by the customer. Moreover, it must be possible for a customer to use the service without submitting to such use of its personal data for advertising or marketing.
2. **Control**: Customers have explicit control of how their information is used.
3. **Transparency**: CSPs must inform customers where their data resides and make clear commitments about how that data is handled.
4. **Accountability**: The standard asserts that any breach of information security should trigger a review by the service provider to determine if there was any loss, disclosure, or alteration of PII.
5. **Communication**: In case of a breach, CSPs should notify customers and keep clear records about the incident and the response to it.
6. **Independent and yearly audit**: A successful third-party audit of a CPS's compliance documents the service's conformance with the standard, and can then be relied upon by the customer to support their own regulatory obligations. To remain compliant, the CSP must subject itself to yearly third party reviews.

A Cloud service provider's adherence to ISO/IEC 27018 controls means the following:

- **Customers will always know where their data may be stored and who is processing that data.** Customers are sometimes subject to information security rules that restrict where data can be stored. Because ISO/IEC 27018 requires certified CSPs to inform customers of the countries where their data may be stored, customers will have the visibility they need to ensure compliance with applicable rules. The standard also requires CSPs to be upfront about the identities of any subcontractors they engage to help with processing PII before customers enter into a contract. And if any of these changes, the CSP is required to inform customers promptly to give them an opportunity to object or terminate their agreement.

- **Customers won't need to worry that the CSP will use their information for marketing and advertising without their consent.** Some CSPs use Cloud customer data for their own independent commercial purposes, including for targeted advertising. To make sure that the customer is always in control, ISO/IEC 27018-compliant CSPs may not use customer data for advertising or marketing purposes absent explicit consent from the customer, which cannot be a condition for receiving the Cloud service. The choice should always be with the customers.

- **Customers can be confident that the CSP will be transparent about its ability to return, transfer, or securely dispose of any personal data at their request.** Customers are often concerned that Cloud services will lead to "lock in," reducing flexibility and nimbleness over time and creating a system captive to a single standard, software tool, or system. ISO/IEC 27018 requires the CSP to implement a policy to allow for the return, transfer and/or secure disposal of personal information, within a reasonable period of time.

- **Customers can rely on ISO/IEC 27018 compliant CSPs to help them to handle access, correction or deletion requests.** EU data protection law imposes certain requirements on CSPs – including allowing individuals whose personal information they hold to access that information, to correct it, and even to delete it. Fulfilling these obligations can be a challenging task where an organization has its data stored in a third-party's Cloud. The compliant providers are required to help customers meet these obligations.

- **Customers can rely on ISO/IEC 27018 compliant CSPs to notify them in the event of a security incident resulting in unauthorized PII disclosure, and to help them comply with their notification obligations**. The compliant providers must specify how quickly they will notify their customers of an unauthorized disclosure of PII and how they will help their customers fulfill their notification obligations. ISO/IEC 27018 also requires CSPs to record the type, timing and consequences of any security incidents, to whom the incident was reported, the steps taken to resolve the incident, etc. – creating a record that will in turn assist customers in meeting their reporting obligations.

- **Customers can be confident that an ISO/IEC 27018 compliant CSP will only comply with legally binding requests for disclosure of their data.** The CSP will reject any requests for the disclosure of customers' personal data that are not legally binding. And if it needs to comply with a legally binding disclosure request (e.g., in relation to criminal investigations), it must always notify the relevant customer, unless prohibited from doing so by law.

- **Customers can rely on independent third party verification of the principles above**. In order to be verified as ISO/IEC 27018-compliant, CSPs must go through a rigorous ISO/IEC 27001 certification process by an accredited independent certification body. **To remain compliant, the CSP must subject itself to yearly third-party reviews**. An ISO/IEC 27018-compliant provider is required to provide customers – prior to commencement of and for the duration of the contract – with independent evidence that controls are implemented in accordance with its policies.