情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

Study on Cloud security in Japan

2011/February

Professor Yonosuke HARADA
INSTITUTE of INFORMATION SECURITY

ITGI Japan

Content

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

ITGI Japan

2 About Survey

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

Institute of Information Security conducted a survey for use of cloud computing survey to companies, government and universities.

One major purpose is to compare risk attitude of ENISA “Cloud Computing Risk Assessment”.

Survey term: 2010 August 1st to 31st
Survey by: mail
Target: Companies, government (local and central), Universities, 4,500
Effective Answer: 316（7%）
Main survey items:

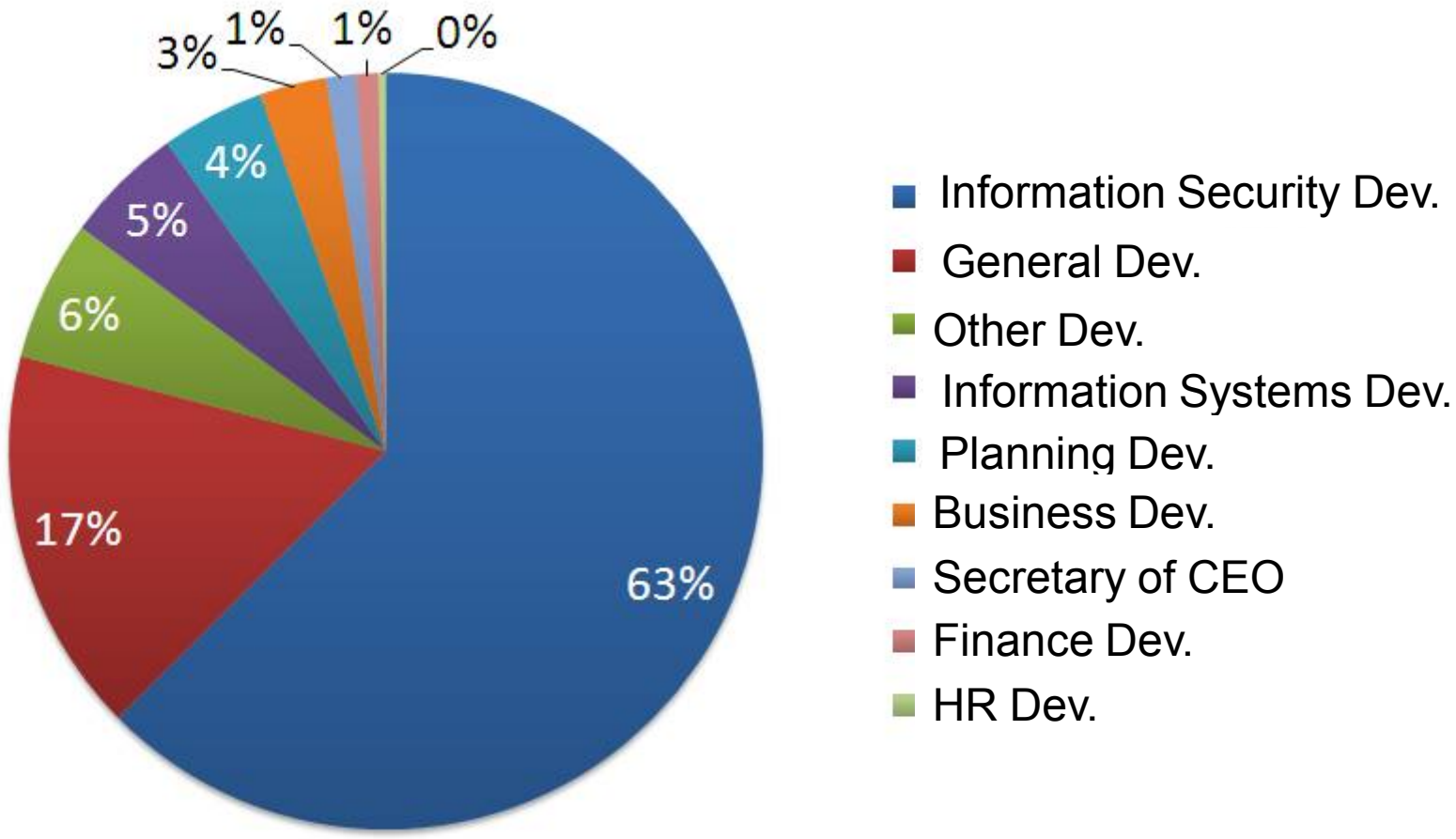
(1) Organization (size, employees, Sales, and PCs)
(2) Intention against cloud computing
(3) Risk evaluation for cloud computing
(4) Selection criteria for cloud provider

ITGI Japan

2.1 Respondent

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

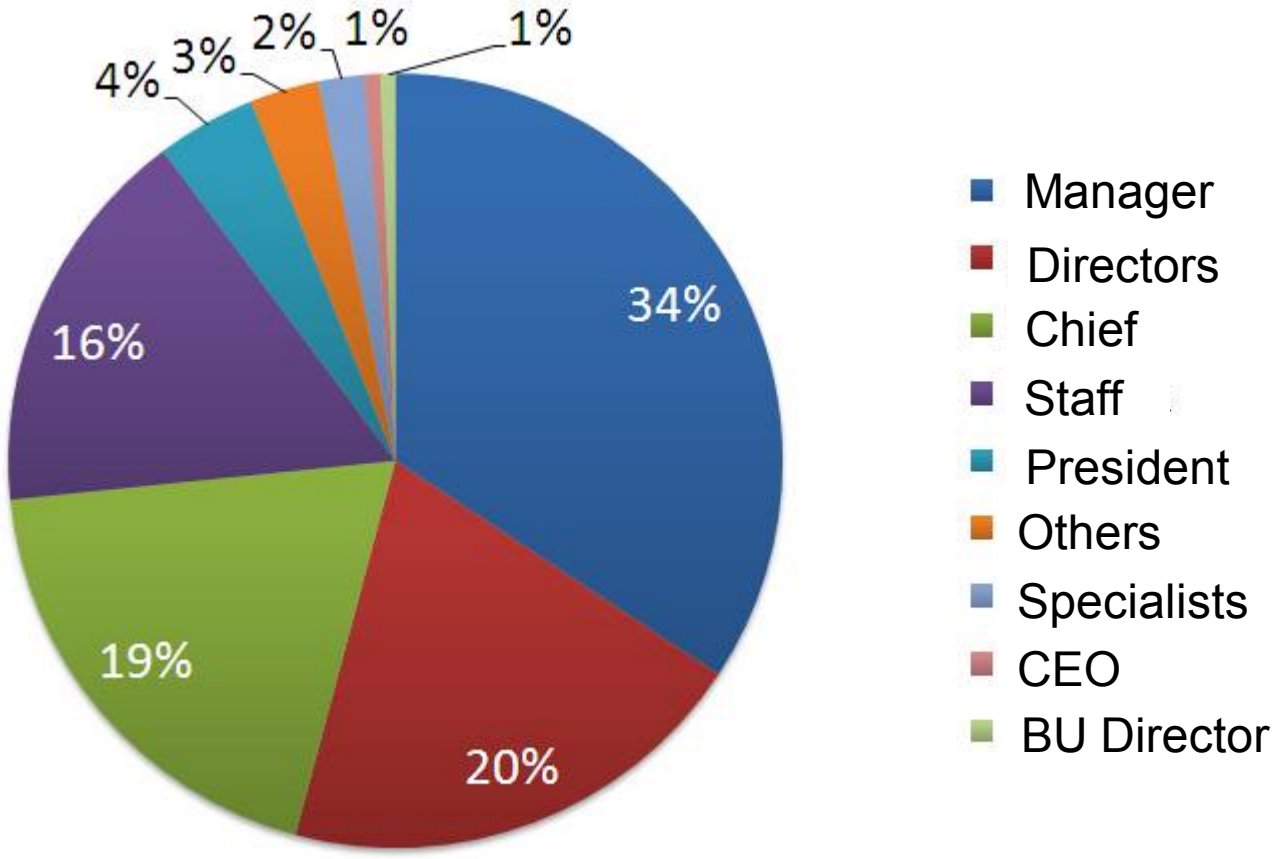
Answer Divisions （N=315）



2.1 Respondent 2

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

Respondent Position (N=312)

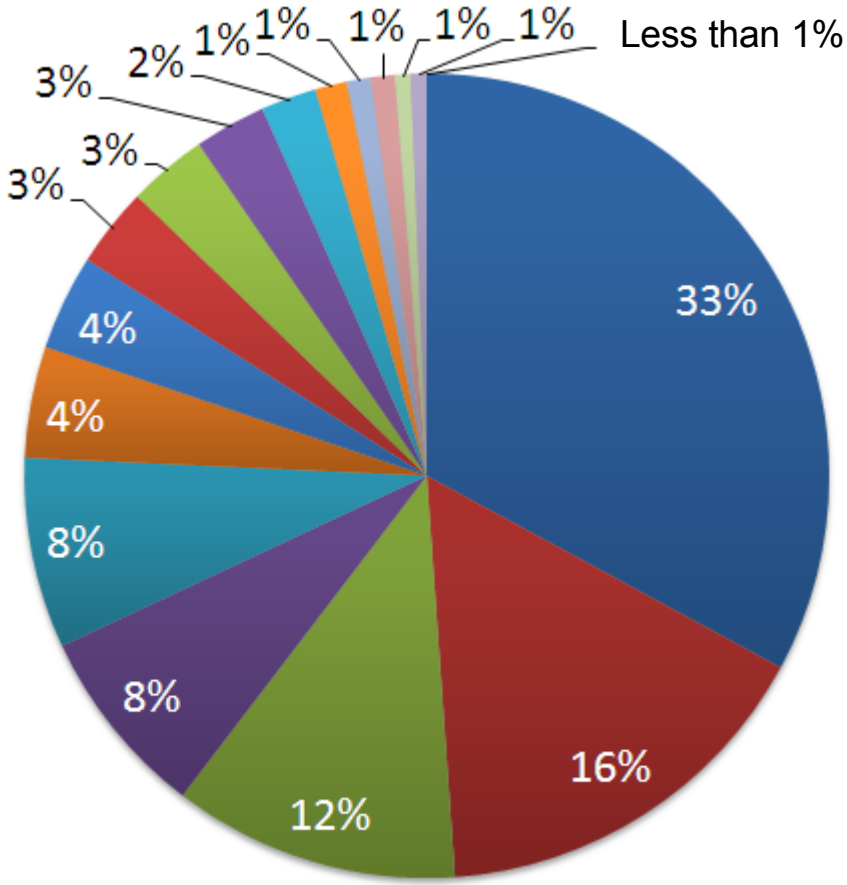


ITGI Japan

2.1 Respondent 3

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

Respondent Industry （N=313）

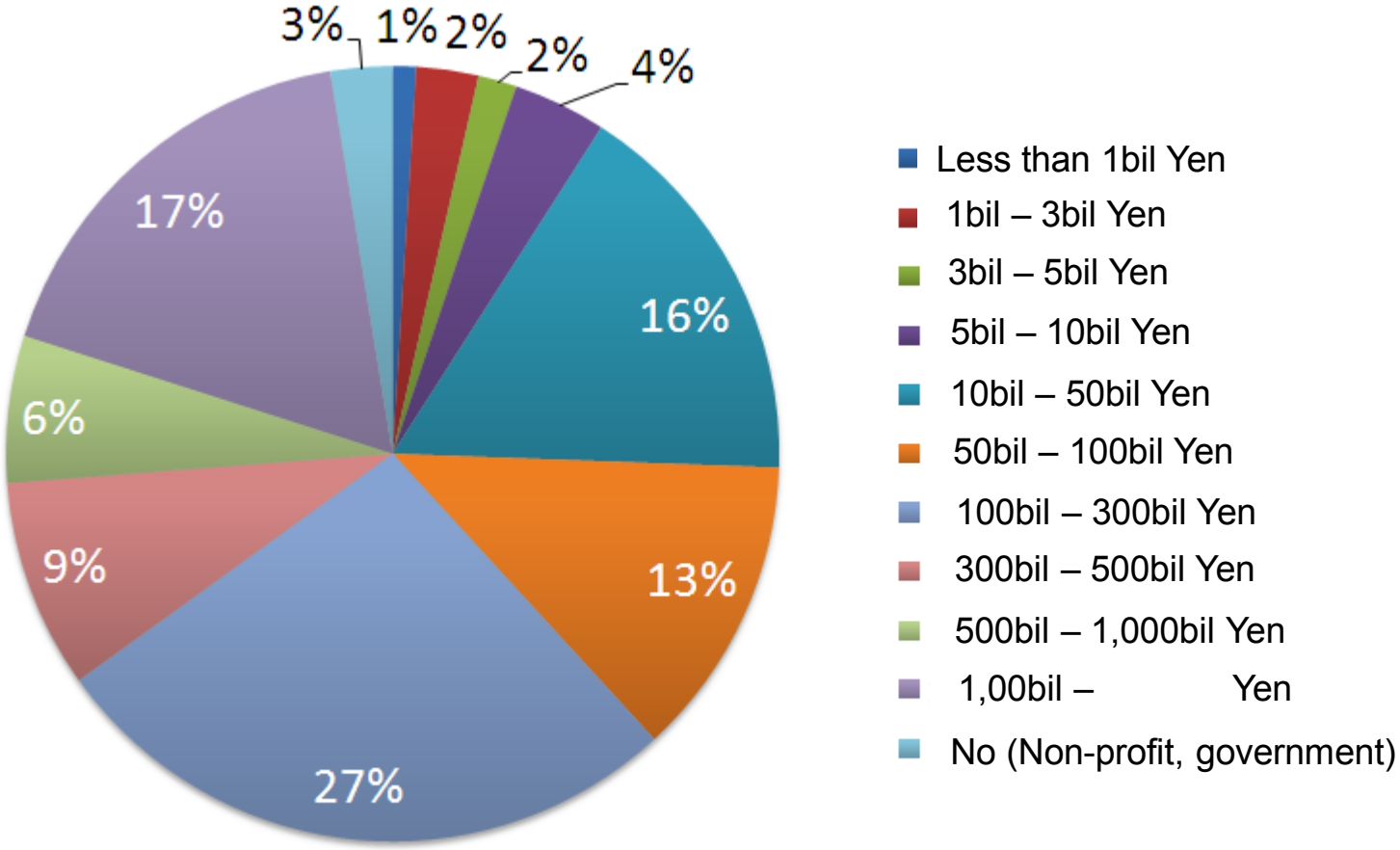


- Manufacturer
- Retail. Wholesale
- University
- Construction
- Information Processing
- Government (central, local)
- Others
- Transportation
- Specialists(consultant, teachers)
- Financial, Securities
- Service, Entertainment, Toiletry,
- Real estate, Leasing
- Hotel, Dining
- Medical, Welfare
- Agriculture, Forestry, Fishery, Mining
- Education, Training

2.1 Respondent 4

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

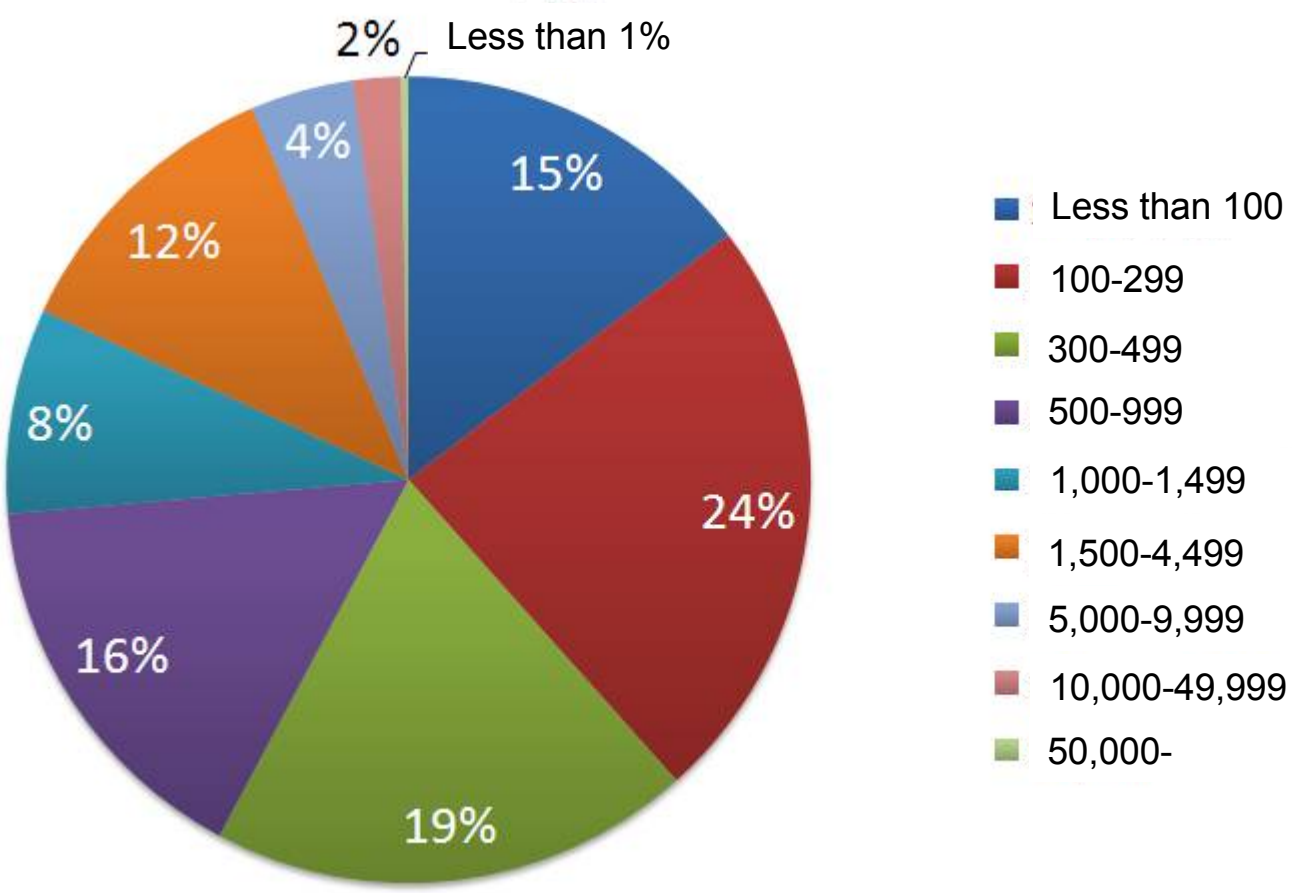
Annual Sales （N=309）



2.1 Respondent 5

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

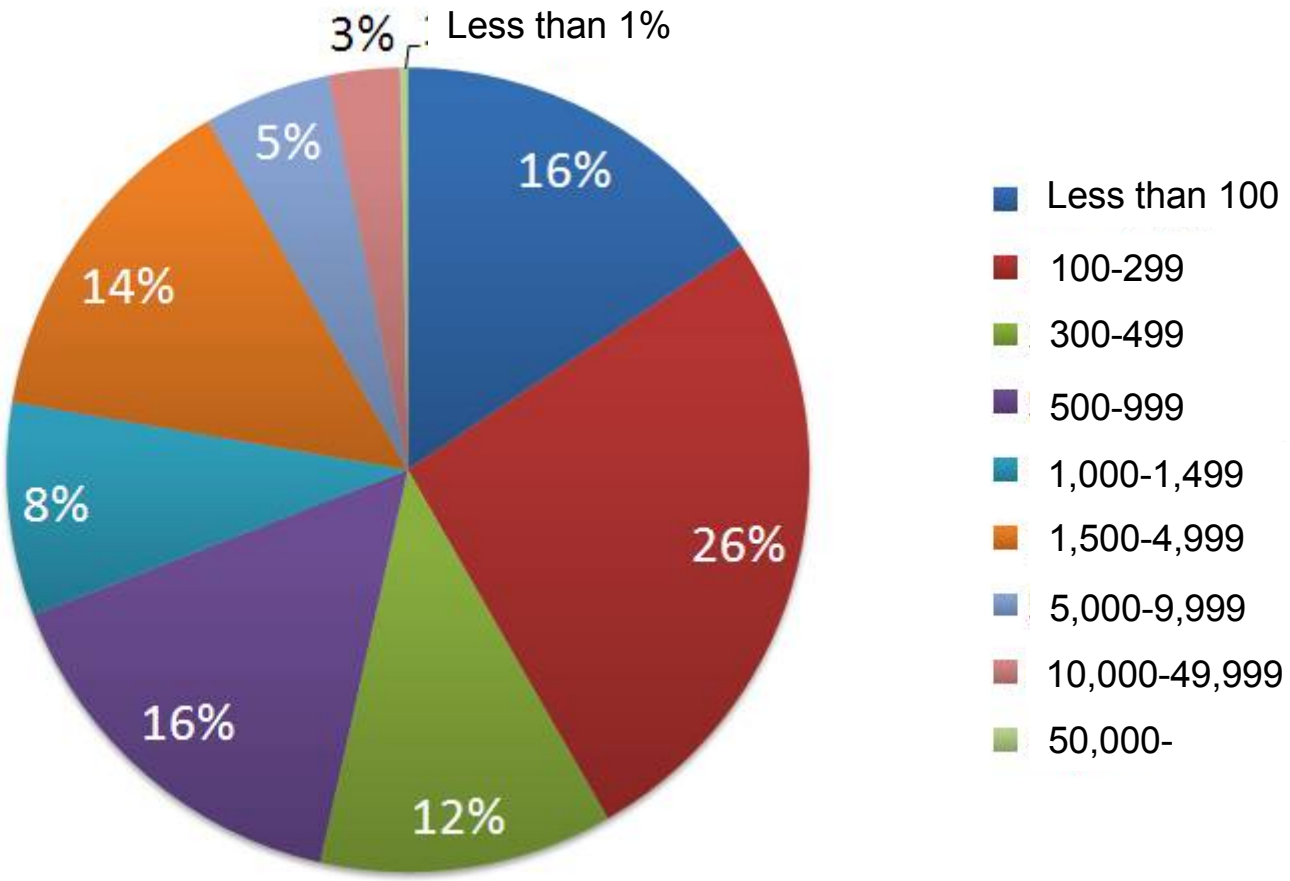
Number of Employeess （N=315）



2.1 Respondent 6

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

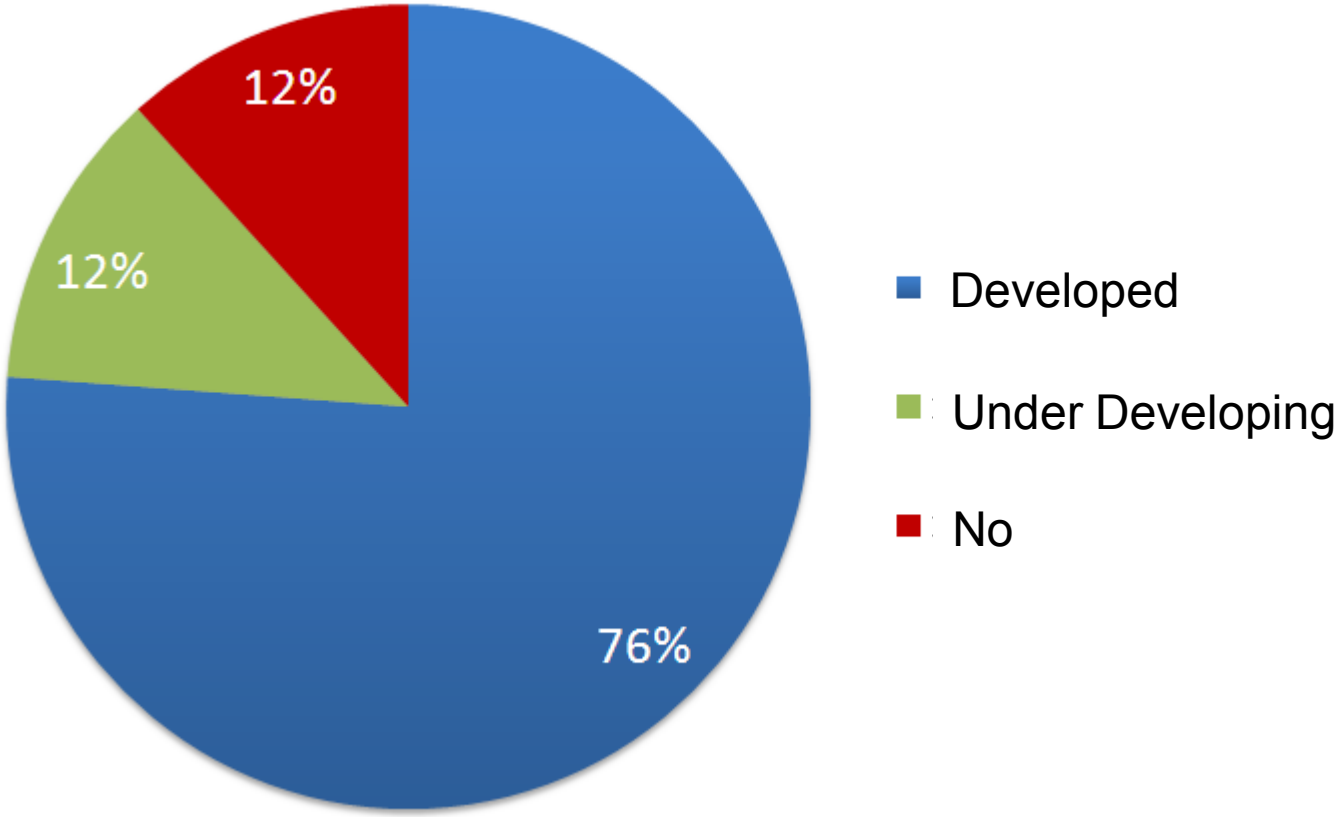
Number of PCs （N=314）



2.1 Respondent 7

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

Security Policy （N=315）



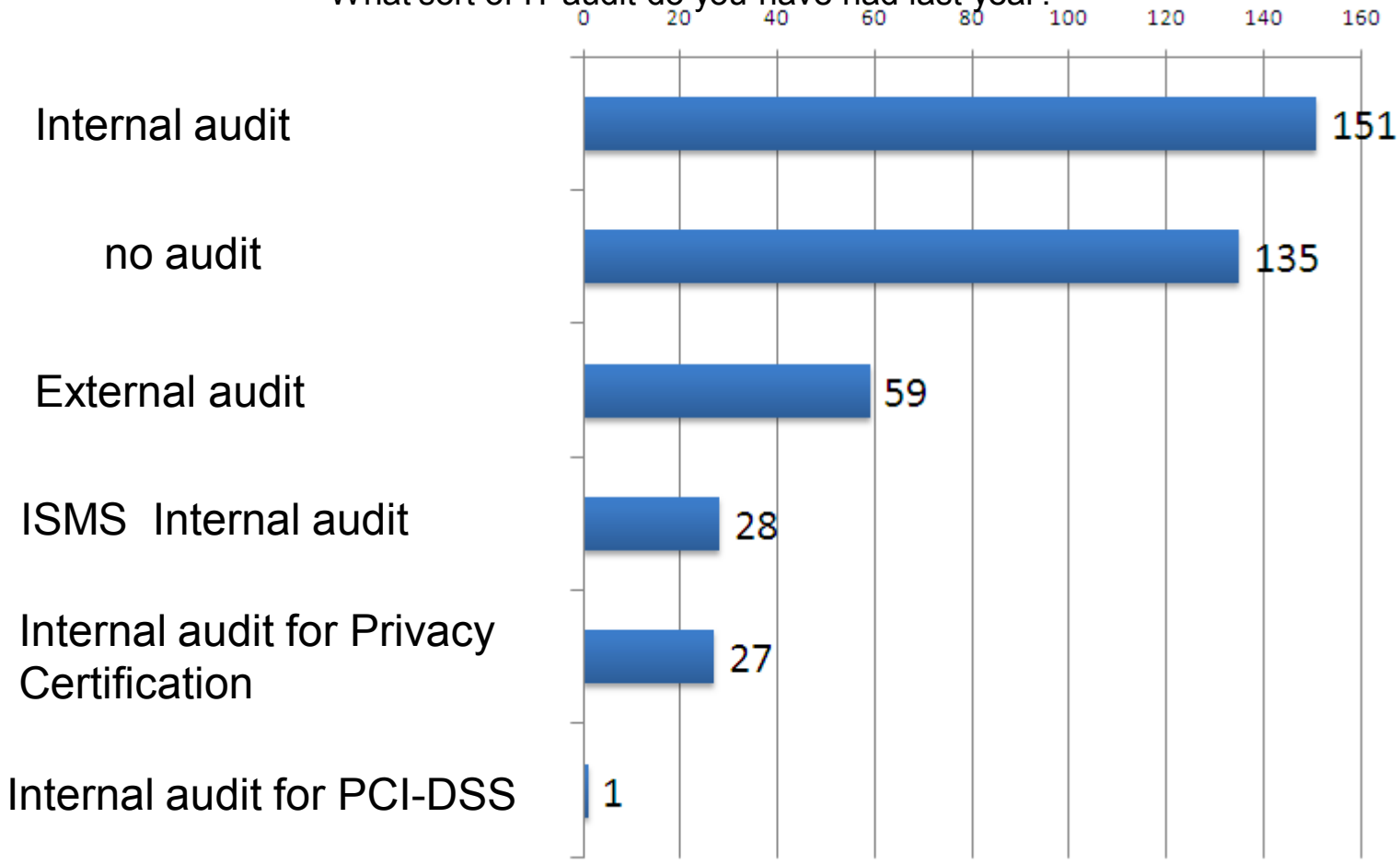
ITGI Japan

2.1 Respondent 8

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

IT audit for cloud computing (N=316)

What sort of IT audit do you have had last year?

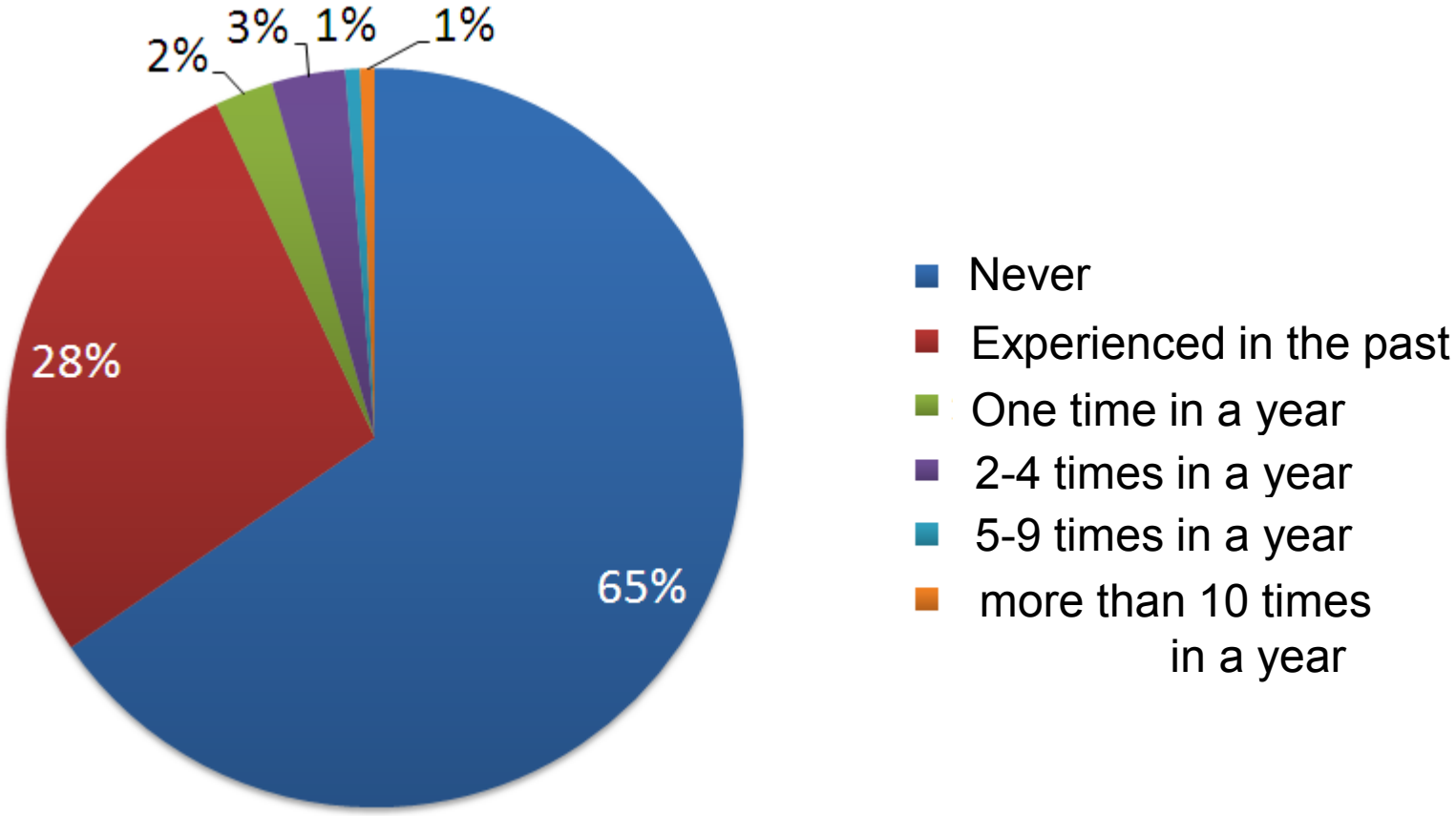


ITGI Japan

2.1 Respondent 9

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

Security Incident and frequency （N=312）

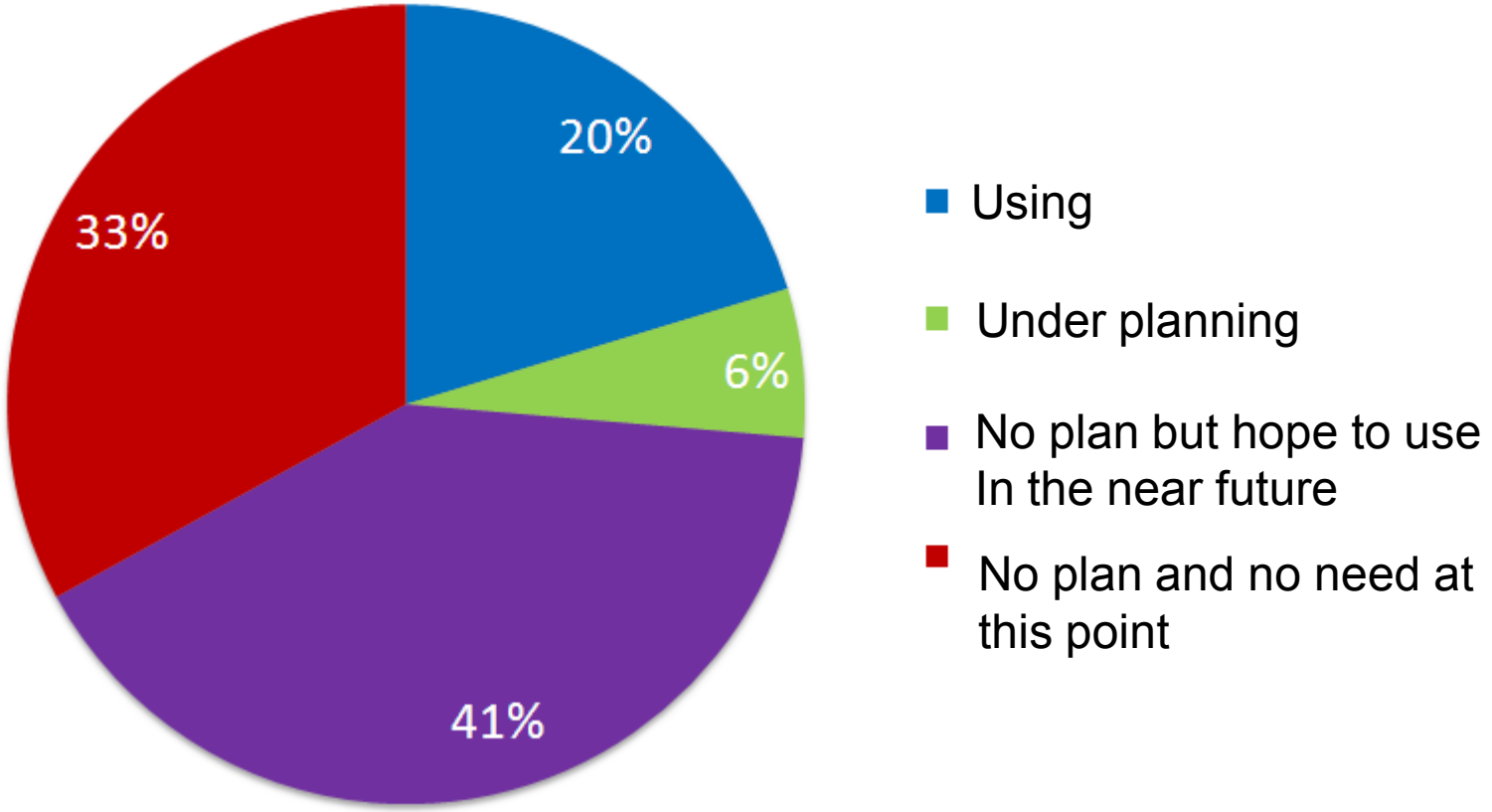


ITG1 Japan

2.2 Cloud computing 1

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

Usage of Cloud Computing （N=315）



20% used and additionally 48% is willing to use

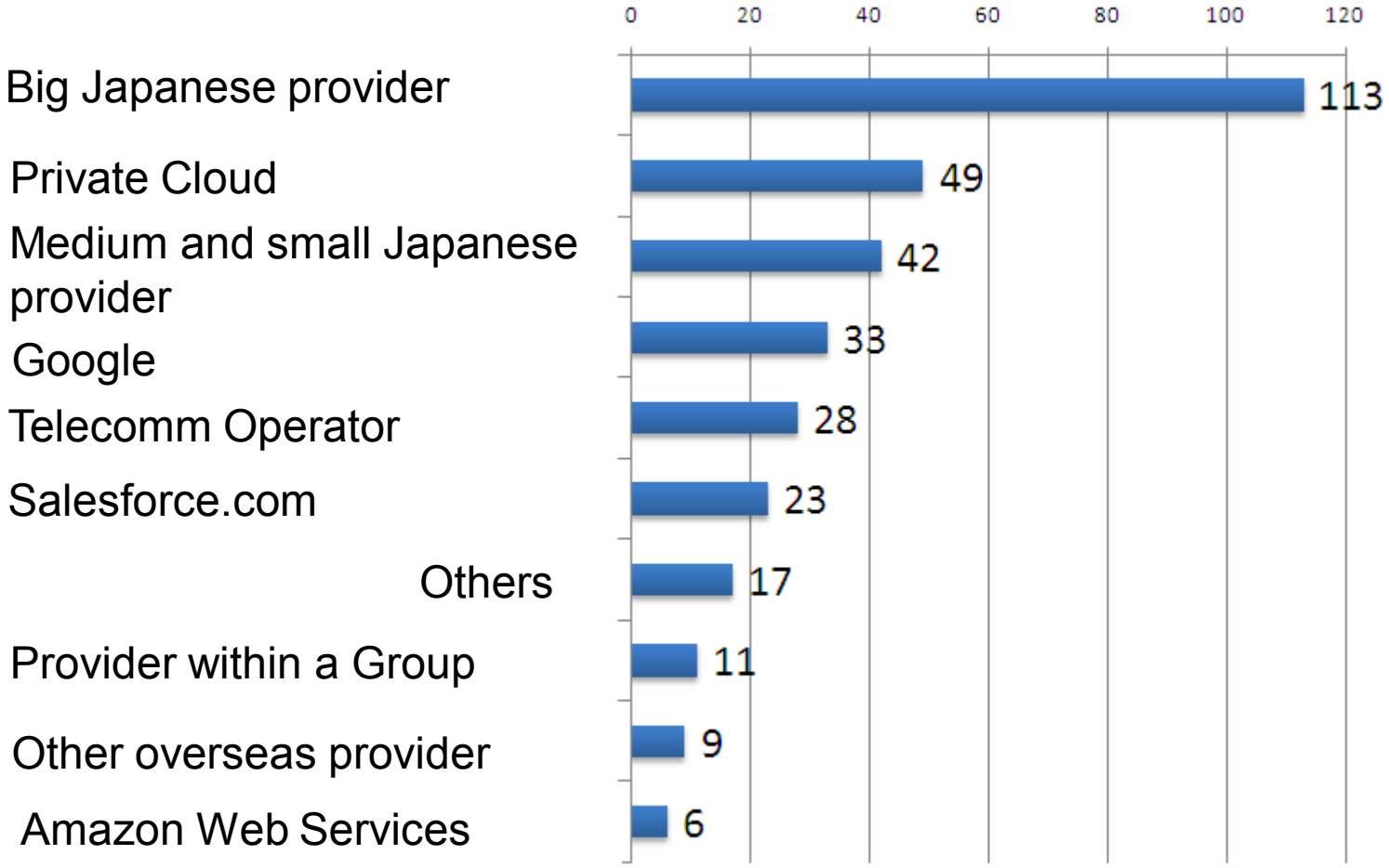
ITGI Japan

2.2 Cloud computing 2

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

Cloud Provider adoption （N=316）

Which cloud provider are you selected or going to adopt?



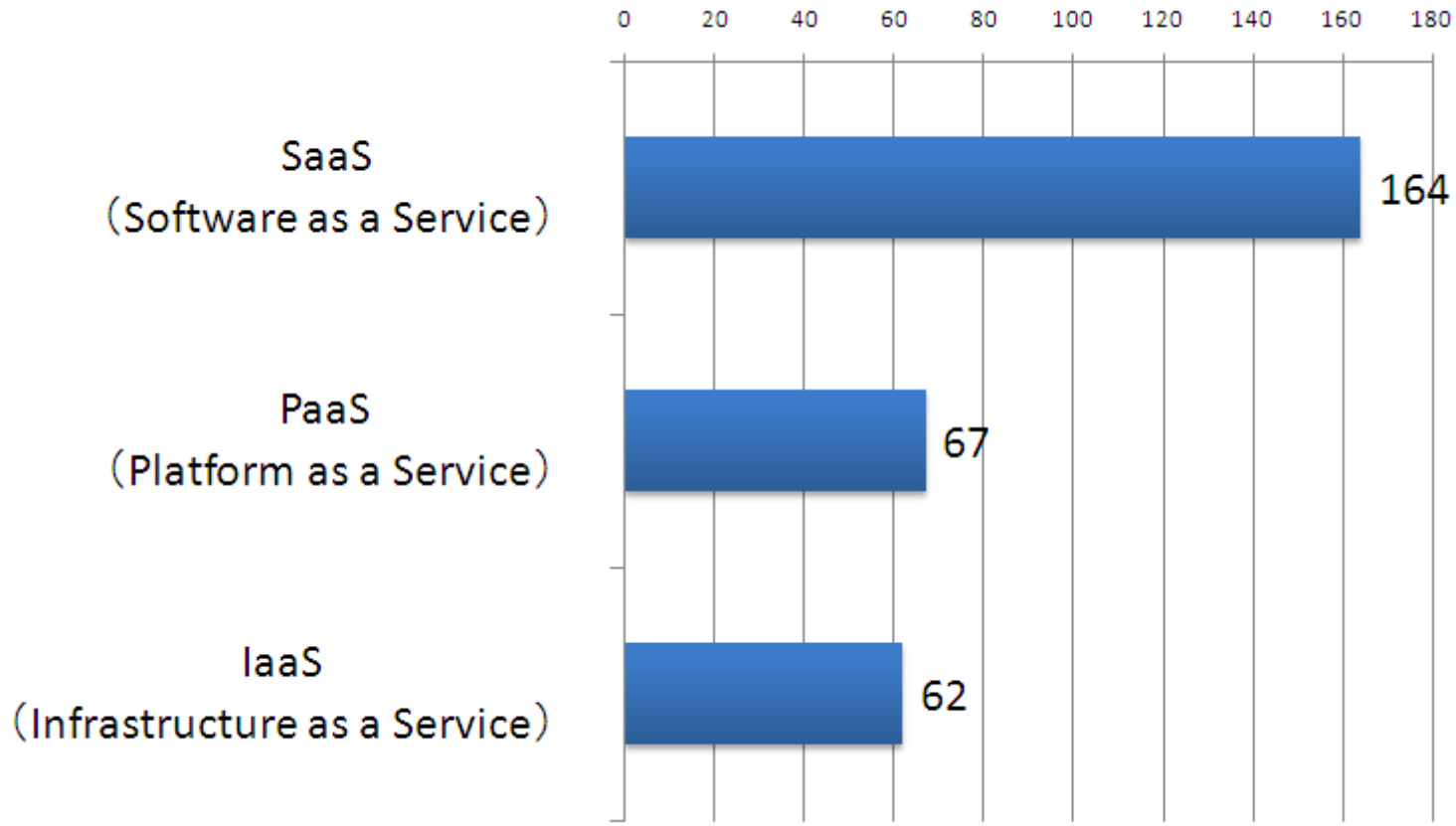
ITGI Japan

2.2 Cloud computing 3

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

Service selection （N=316）multiple answer

Which kind of cloud services are you selected or going to adopt?



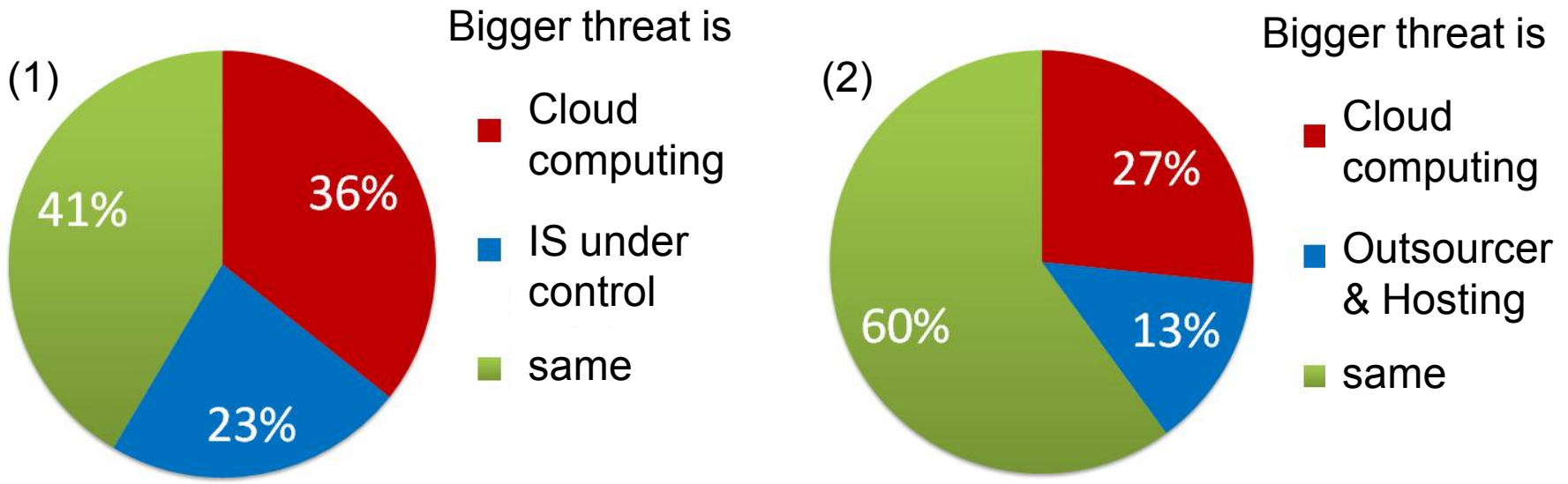
ITGI Japan

2.2 Cloud computing 4

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

Which is bigger threat ? （N=311）

(1) Information Systems (under control) or cloud computing
(2) Outsourcing (including Hosting) or cloud computing



Users feel a little bigger threat in Cloud computing than IS under control or outsourcer.
However, many think similar threat.

ITGI Japan

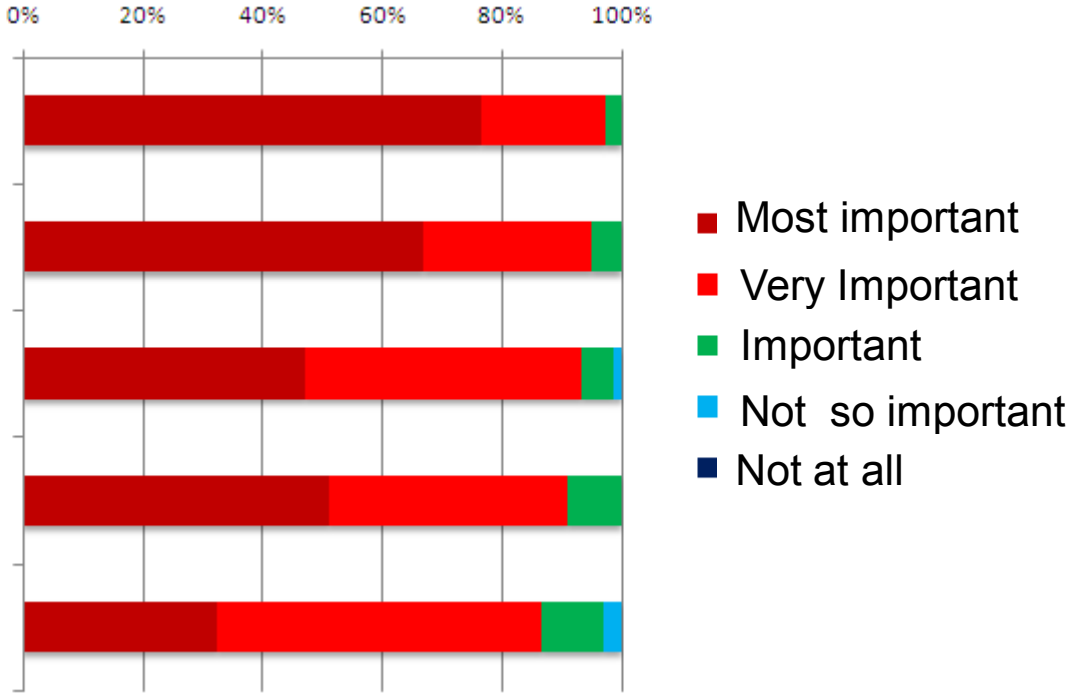
2.3 Cloud computing provider adoption 1

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

Important items are for provider adoption

Top five items are listed（N=316）

1. Incident response
2. Monthly charge
3. Technical support
4. Initial Cost is low
5. Technical Experience



ITGI Japan

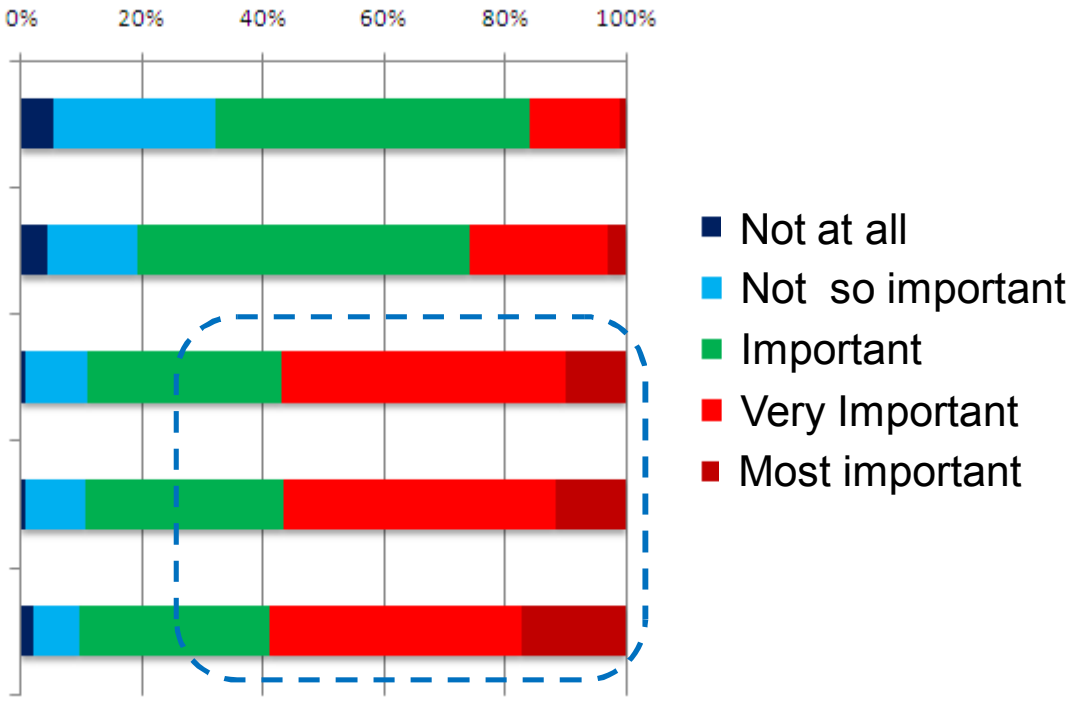
2.3 Cloud computing provider adoption 2

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

Important items are for provider selection

Bottom five items are listed（N=316）

1. Advertisement
2. Seminar or events
3. Brand name
4. Proposals
5. Selection of



ITGI Japan

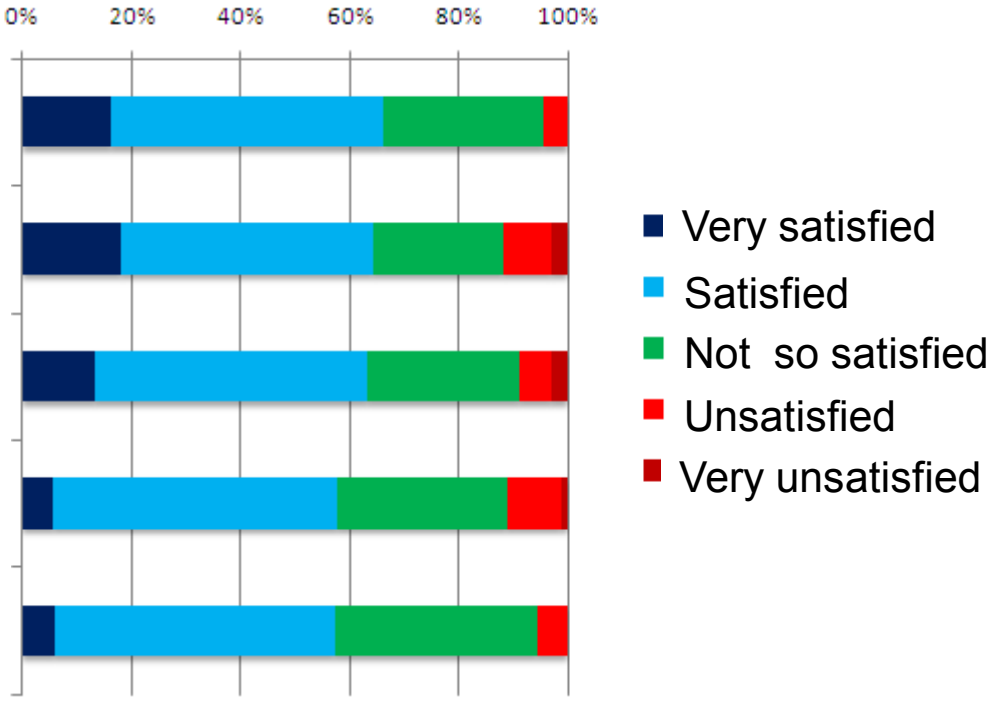
2.3 Cloud computing provider adoption 3

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

User Satisfaction

Top five items are listed（N=70）

1. Company profile
2. Initial charge
3. Ccompany experience
4. Incident Response
5. Technical Experience



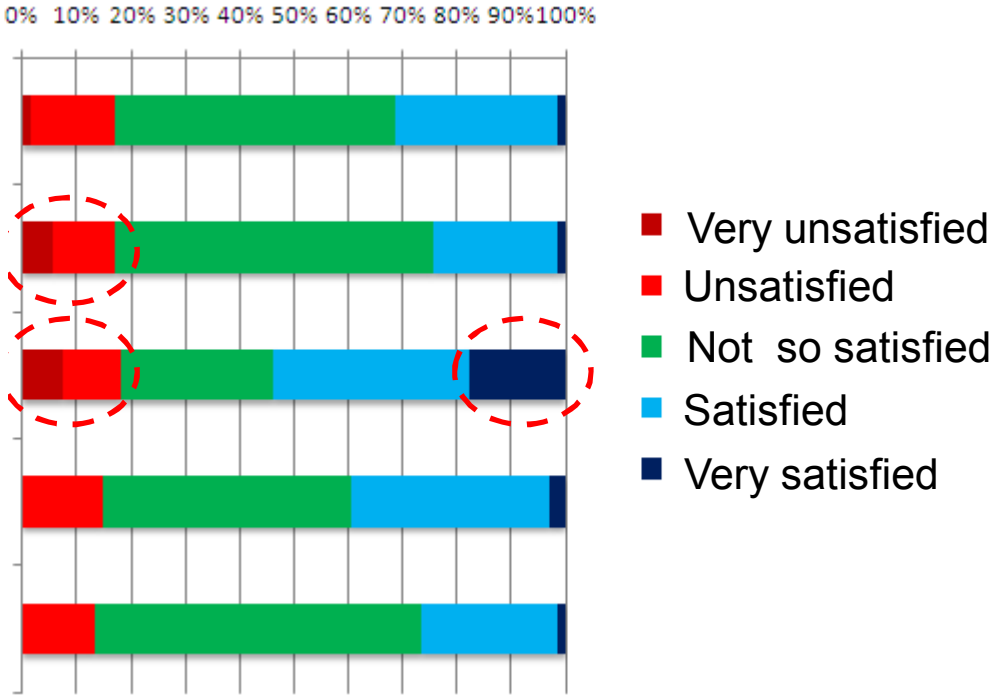
ITGI Japan

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

Satisfaction on Cloud Service Used

Top five “unsatisfied” items are listed（N=70）

1. Speedy implementation
2. Quality of Proposal
3. Reasonable Running Cost
4. Reporting for Service
5. Audit



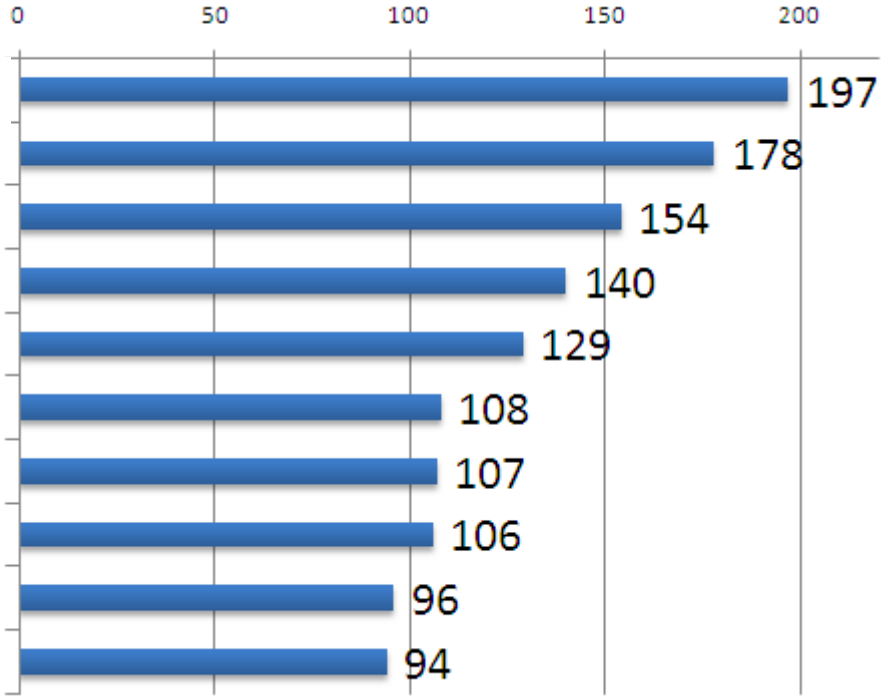
Users require provider proposal of cloud service
Some user does not satisfy current service

ITGI Japan

Cloud provider SLA

Top ten SLA items for adoption of cloud provider（N=316）multiple answer

1. Alternative service of major incident
2. Service up time
3. Average recovery time
4. Service Availability
5. Service hours (help desk etc.)
6. Backups methodology
7. Retention Period of backups
8. Average response time
9. Logging capability
10. Fault reporting process



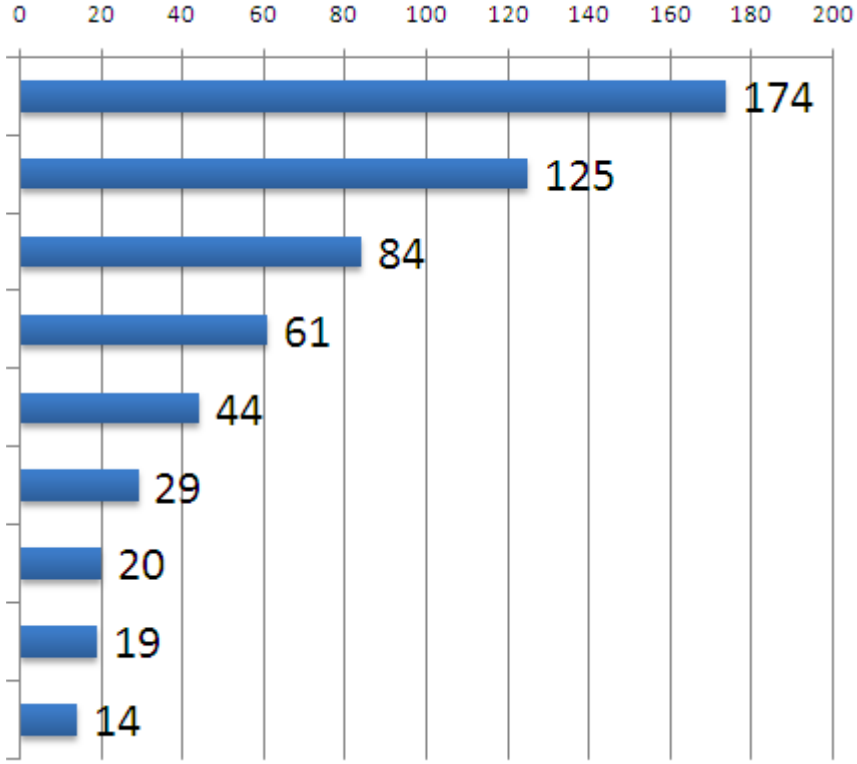
ITGI Japan

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

Third party certification of guideline

（N=316）multiple answer

1. ISMS certification
2. Privacy certification （domestic)
3. BS25999（BCM) certification （BSI)
4. Disclosure for ASP/SaaS service
5. SAS70-type2 and similar by CPA
6. PCIDSS certification
7. SysTrust certification
8. CSA guidelines
9. Others



ITGI Japan

3 Comparison with ENISA result (1)

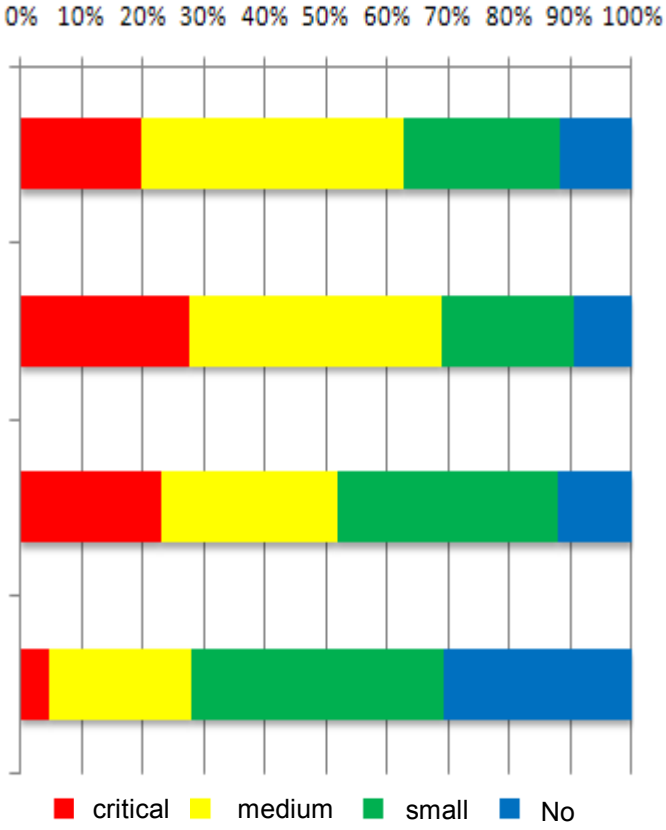
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

Organizational Risk 1

Survey result shows percentage of risk assessment by respondent

Risk	ENISA
LOCK-IN Data format for storage, conversion tool is not provided Application lock-in	High
LOSS OF GOVERNANCE All business processes are under control of Cloud Provider and cannot change or manage by user	High
COMPLIANCE CHALLENGES If cloud provider violate laws and regulations, user may automatically challenge compliance.	High
LOSS OF BUSINESS REPUTATION DUE TO CO-TENANT ACTIVITIES Business competitiveness may harm because of user reputation will become no difference based on cloud service	Medium

Survey Result



Japanese organisations do not think that "Lock in", "Loss of governance" and "Compliance" are not so serious for their business.

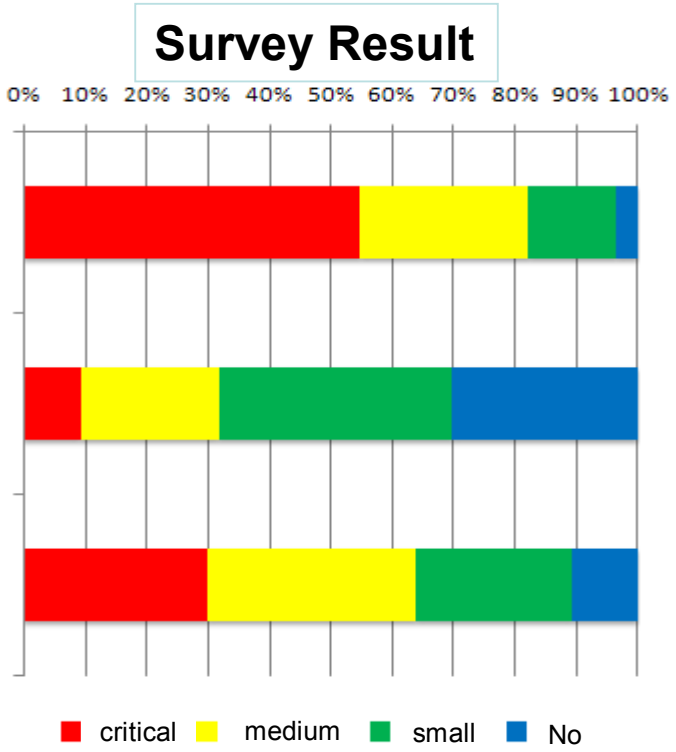
ITGI Japan

3 Comparison with ENISA result (1)

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

Organizational Risk 2

Risk	ENISA
CLOUD SERVICE TERMINATION OR FAILURE Organization may not continue service, if cloud provider stops operation or service.	Medium
CLOUD PROVIDER ACQUISITION Cloud provider is acquired by competitor and may not continue service	Medium
SUPPLY CHAIN FAILURE Cloud service may stop or change due to changes or outage of other cloud service provider.	Low



Japanese organisations thinks it more serious on service continuation than EU organization. However, they are optimistic on acquisition.

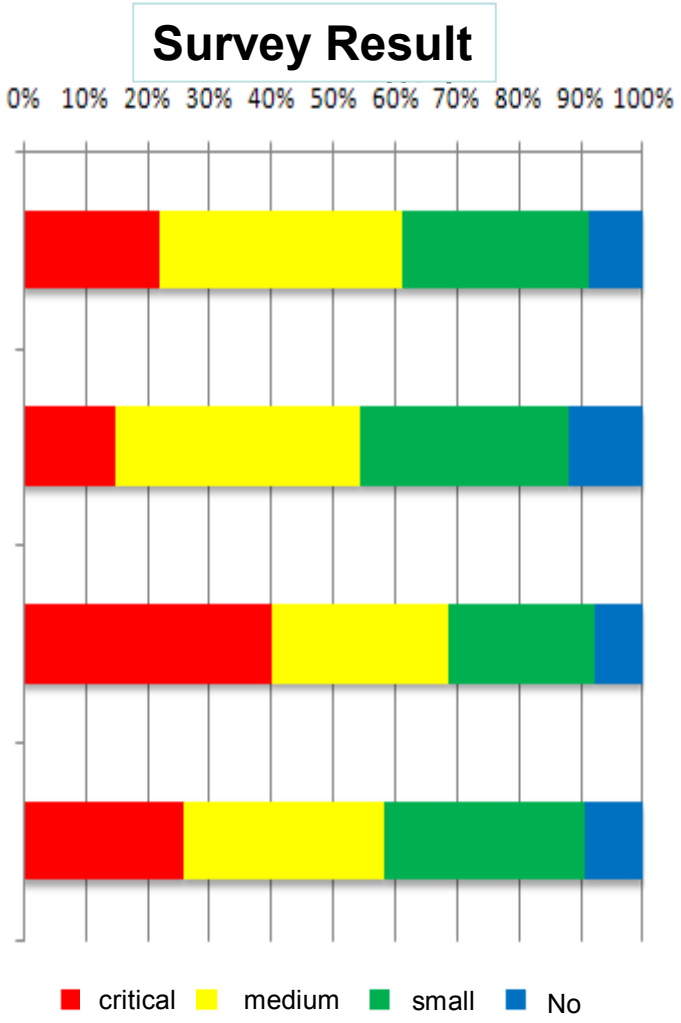
ITGI Japan

3 Comparison with ENISA result (2)

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

Technical Risk 1

Risk	ENISA
RESOURCE EXHAUSTION Inaccurate modeling of resources or inaccurate resources allocation algorithms may degrade service	Medium
ISOLATION FAILURE Failure of mechanisms separating storage, memory, routing, and even reputation between different tenants of the shared infrastructure	High
CLOUD PROVIDER MALICIOUS INSIDER - ABUSE OF HIGH PRIVILEGE ROLES The malicious activities of an insider could potentially have an impact on all kind of services, and therefore indirectly on the organization's reputation.	High
MANAGEMENT INTERFACE COMPROMISE Customer management interfaces are Internet accessible and increased risk when combined with remote access and web browser vulnerabilities.	Medium



Japanese users feel "Malicious insider abuse" like EU but do not feel seriously for isolation failure.

ITGI Japan

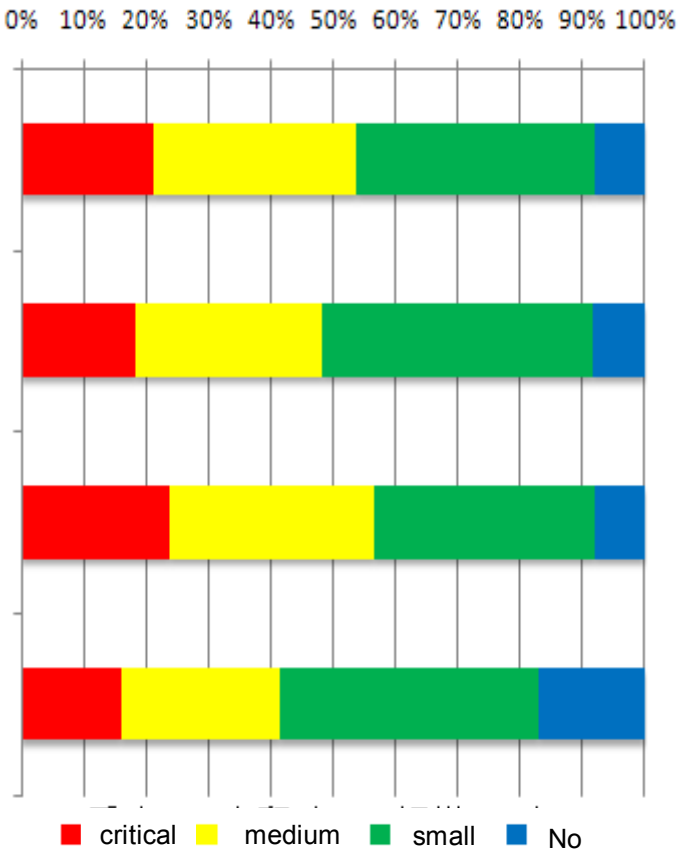
3 Comparison with ENISA result (2)

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

Technical Risk 2

リスク	ENISA
INTERCEPTING DATA IN TRANSIT **DATA LEAKAGE ON UP/DOWNLOAD, INTRACLOUD** Data are transferred more in transit and distributed across multiple physical machines.	Medium
INSECURE OR INEFFECTIVE DELETION OF DATA Request to delete a cloud resource is made, this may not result in true wiping of the data.	Medium
DISTRIBUTED DENIAL OF SERVICE (DDOS) DDoS to other user of cloud provider may impact	Medium
ECONOMIC DENIAL OF SERVICE (EDOS) EDoS destroys economic resources; the worst case scenario would be the bankruptcy of the customer or a serious economic impact.	Medium

Survey Result



Technical risks are similar to Japanese users and EU users.

ITGI Japan

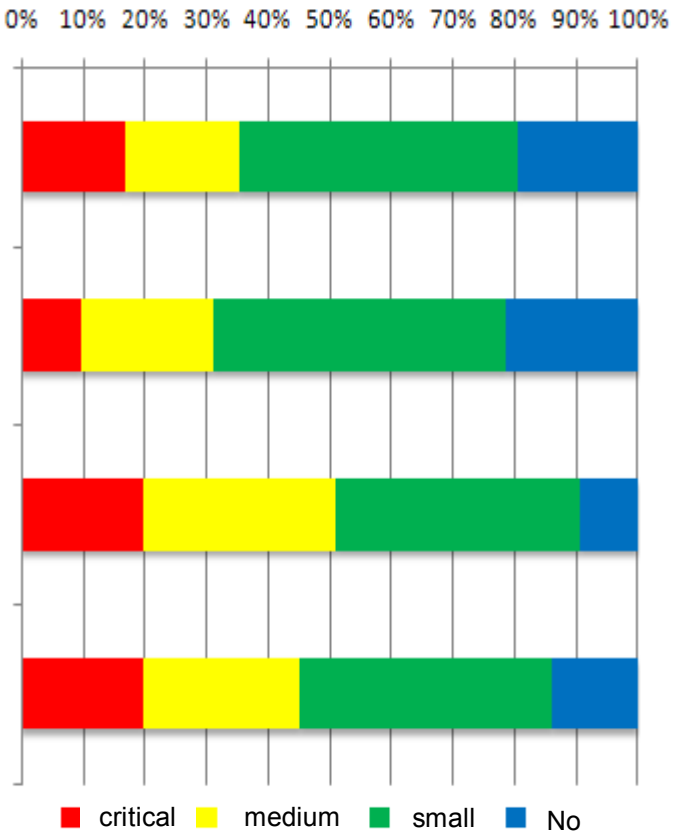
3 Comparison with ENISA result (2)

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

Technical Risk 3

Risk	ENISA
LOSS OF ENCRYPTION KEYS Disclosure of secret keys or passwords to malicious parties may impact to loss or leakage of important data	Medium
UNDERTAKING MALICIOUS PROBES OR SCANS Malicious probes or scanning are indirect threats to the assets.	Medium
COMPROMISE SERVICE ENGINE Provider service engine have vulnerabilities and is prone to attacks or unexpected failure.	Medium
CONFLICTS BETWEEN CUSTOMER HARDENING PROCEDURES AND CLOUD ENVIRONMENT Hypervisor, or service engine may have vulnerabilities and is prone to attacks or unexpected failure.	Low

Survey Result



Technical risks are similar to Japanese users and EU users.

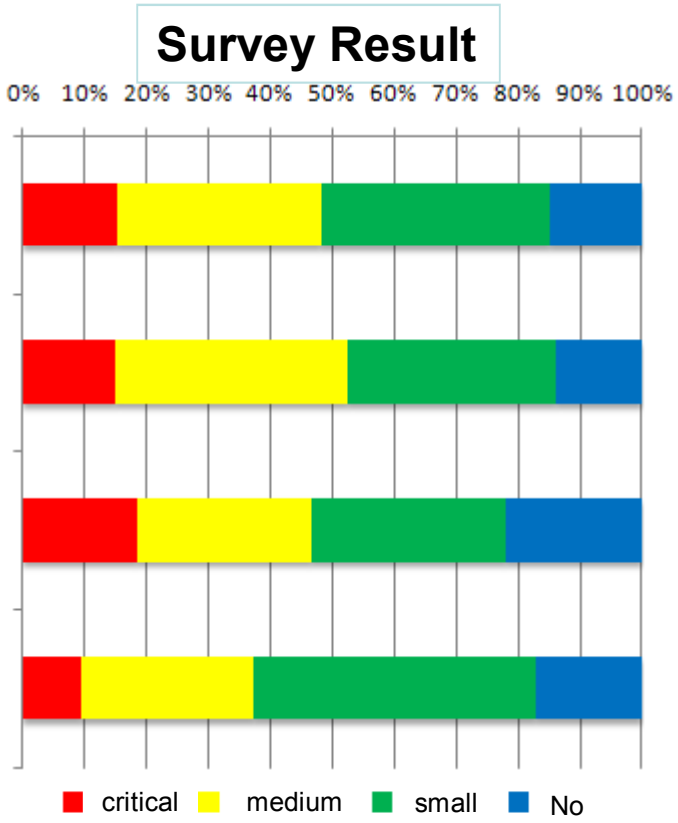
ITGI Japan

3 Comparison with ENISA result (3)

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

Legal Risk 1

リスク	ENISA
SUBPOENA AND E-DISCOVERY As a result of subpoena, storage as well as shared hardware is at risk of the disclosure to unwanted parties	High
User is not able to protect or preserve of evidence in the cloud when requested from Authorities	High
RISK FROM CHANGES OF JURISDICTION User data may be held in multiple jurisdictions, some of which may be high risk	High
LICENSING RISKS Licensing conditions and online licensing checks may become unworkable in a cloud environment.	Medium



EU organisations feels more legal risk than Japanese organisations.

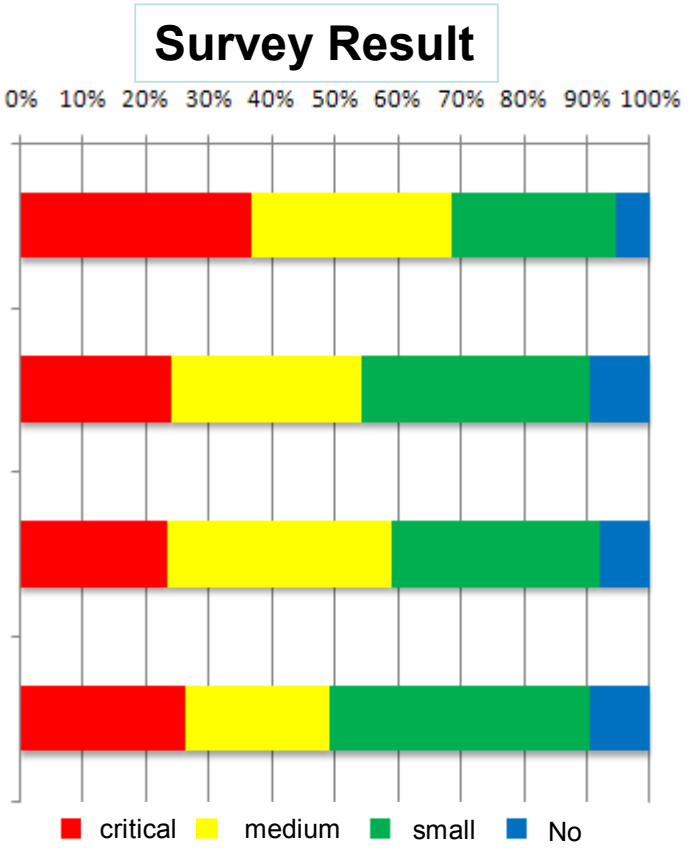
ITGI Japan

3 Comparison with ENISA result (4)

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

Common Risk 1

リスク	ENISA
NETWORK BREAKS Potentially thousands of customers are affected at the same time.	Medium
NETWORK MANAGEMENT Provider network may not be managed properly and capacity and connection failure may impact to users.	High
MODIFYING NETWORK TRAFFIC Network traffic between user and provider may not be modified in case of network failure.	Medium
PRIVILEGE ESCALATION Potentially root authority has been seizure and data may be disclosed or modified.	Medium



Japanese organisations are not seriously consider network issues.
This is because Japanese telecom operator provide excessive quality services.

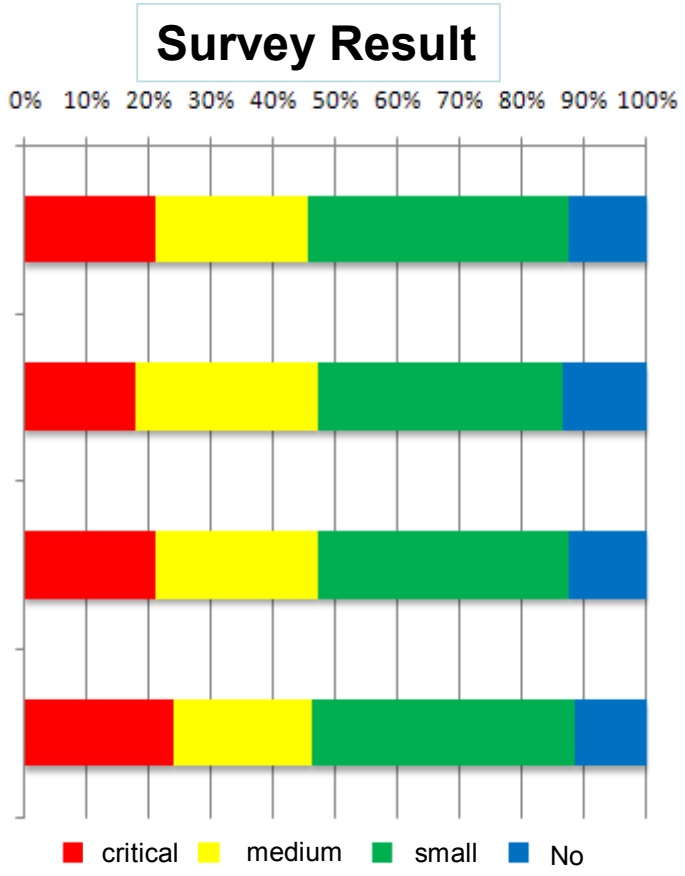
ITGI Japan

3 Comparison with ENISA result (4)

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

Common Risk 2

リスク	ENISA
SOCIAL ENGINEERING ATTACKS Provider may be attacked “social engineering” and may disclose user data or information.	Medium
LOSS OR COMPROMISE OF OPERATIONAL LOGS Provider may lose or compromise user logging data.	Low
LOSS OR COMPROMISE OF SECURITY LOGS Provider may lose or compromise security logs.	Low
BACKUPS LOST, STOLEN Provider may lose or compromise backed up files.	Medium



Common risks are regarded less for Japanese users than EU users.

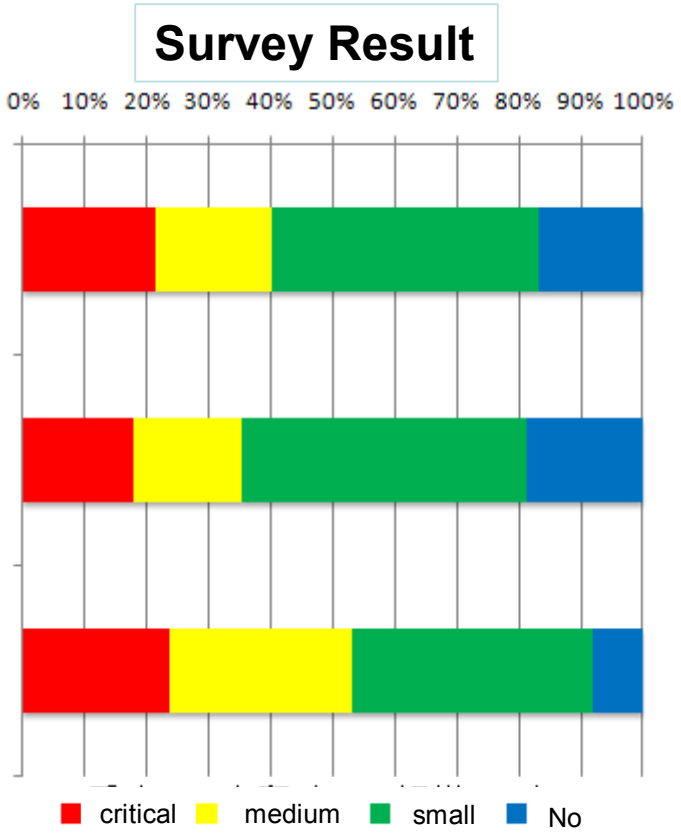
ITGI Japan

3 Comparison with ENISA result (4)

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

Common Risk 3

リスク	ENISA
UNAUTHORIZED ACCESS TO PREMISES Provider facilities may be invaded and infrastructures may be compromised.	Low
THEFT OF COMPUTER EQUIPMENT Provider equipment (storage) may be stolen and user data may be compromised.	Low
NATURAL DISASTERS Provider may not continue providing services due to natural disasters (flood, earthquake, volcano, etc).	Low



Japanese organisations are exposed more natural distress than EU organisations, but do not evaluate high risk.

ITGI Japan

4 Conclusion

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- Anxiety for cloud computing
  - Many issues are similar and common among Japan and EU organisations.
  - Japanese organisations seek quality of services (non stop, guarantied) to cloud provider.
  - European organisations utilize cloud computing with quality for money
  - European organisations feel higher risk on legal, lock-in, and loss of governance than Japanese organisations.
- Expectation to cloud computing
  - Japanese organization should regard cloud computing as the new service category lower quality in good price.

ITGI *Japan*

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

This Study is Supported by ITGI-Japan

Contact:
Yonosuke Harada, Professor Institute of Information Security,
E-mail: Yo-harada@iisec.ac.jp

ITGI Japan