Help! We're Drowning in Lake Assurance:

Supply Chain Security Challenges and a New Frontier

Fiona Long

MBA, CISM, LA27001, IRAP Assessor

Director & Founder

fiona.long@infosecassure.com.au

INFOSECASSURE

Risky Business

Homewares and Domestic Goods

Heating, ventilation, and air conditioning (HVAC) supplier

Autonomous Vehicles

Software developer

Pharmaceutical

Manufacturer

Banking

Website builders

Petrol / Gas

Gas Supplier

Laptops

Computer manufacturer

Supplier Lifecycle and Risk

- Engage / Buy
- Design / Implement
- Governance
- End

Supply Chain Risk

vs

Cyber Supply Chain Risk Management (C-SCRM)

Know Your Suppliers

- Business context
- Users
- Data Classification
- Technology contex
- Location of service
- Stakeholders

Potential Impact if a cyber security event caused loss of:

- Confidentiality and/or Integrity of data assets
- Availability of system

TYPE

RISK

Supplier profiles drive requirements

TYPE RISK	Managed Service Provider	Software Provider	Temp Service Provider
Security Policy and Framework	✓	✓	✓
Harmful Code	✓	✓	
Personnel	✓		✓
Fourth parties	✓		
Data Sovereignty	✓		
Incident Detection / Reporting	✓		✓
Periodic Reporting	✓		
DR/BCP	✓		
Assurance and Testing	✓	✓	✓

Buyer vs Supplier power

INFOSECASSURE

	🏢 🏛	🏪 🏢
Economic resources	$ $ $ $ $	$
Clients and Stakeholders	🏢 🏛 🏢 🏪	🏢 🏢 🏪
Technology Types	☁ 🖥	☁ 🖥
Regulations and Standards	⊕ ⊕ ⊕	⊕
Risk and Compliance Governance	👤 👤 👤 👤	
Legal Resources	👤 👤 👤 👤	👤
IT Resources	👤 👤 👤 👤	👤
Suppliers	🏢 🏢 ☁	🏢 🏢 ☁

Security Questionnaire Origin Story

Industry and Business Standards, Regulations and Frameworks

Companies

Corporations Act 2001
SOC 1
ASIC Report 429
Consumer Data Right Act 2019.

Government

ISM
Essential Eight
PSPF / DSPF
(CISC) - Hosting Cert Framework (DTA)
T4

Health

Health Records and Information Privacy Act
HIPAA

Security

ISO 27001...
ASVS
SCO 2

Personal Information

Privacy Act
EU GDPR
CCPA
PIPEDA

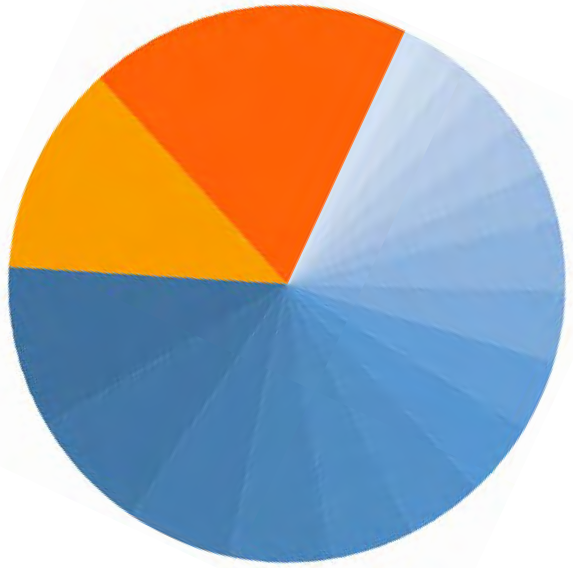
Banking

IAPRA CPS 234
APRA CPS 231
PCI DSS

Questionnaire Focus Differs per Industry

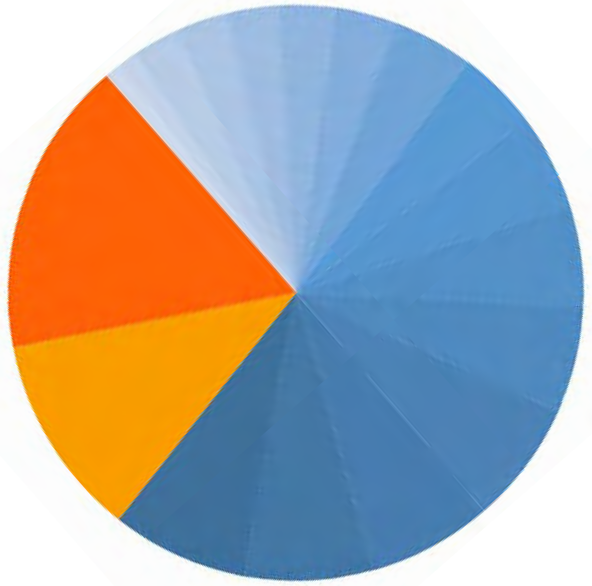
InfoSecAssure research study of 6,660 unique cyber security questions asked.

Government



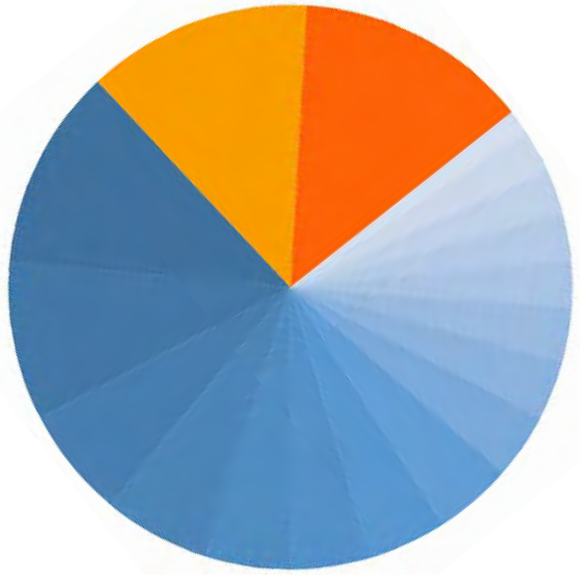
n = 824 questions

Finance



n = 2,822 questions

Law Firms



n = 3,014 questions

Top 2 Practice Areas

- **Physical and Environmental Security (18%)**
- Network Security and Content Filtering (12%)

- **Identity and Access Management (17%)**
- Network Security and Content Filtering (11%)

- **Corporate Governance (14%)**
- Network Security and Content Filtering (13%)

The Good, the Bad the Ugly

Stolen

How will you encrypt Bank A 's data?
(received from bank B)

Intrusive

Please send over a copy of all your vulnerability scanning reports?

Unreasonable

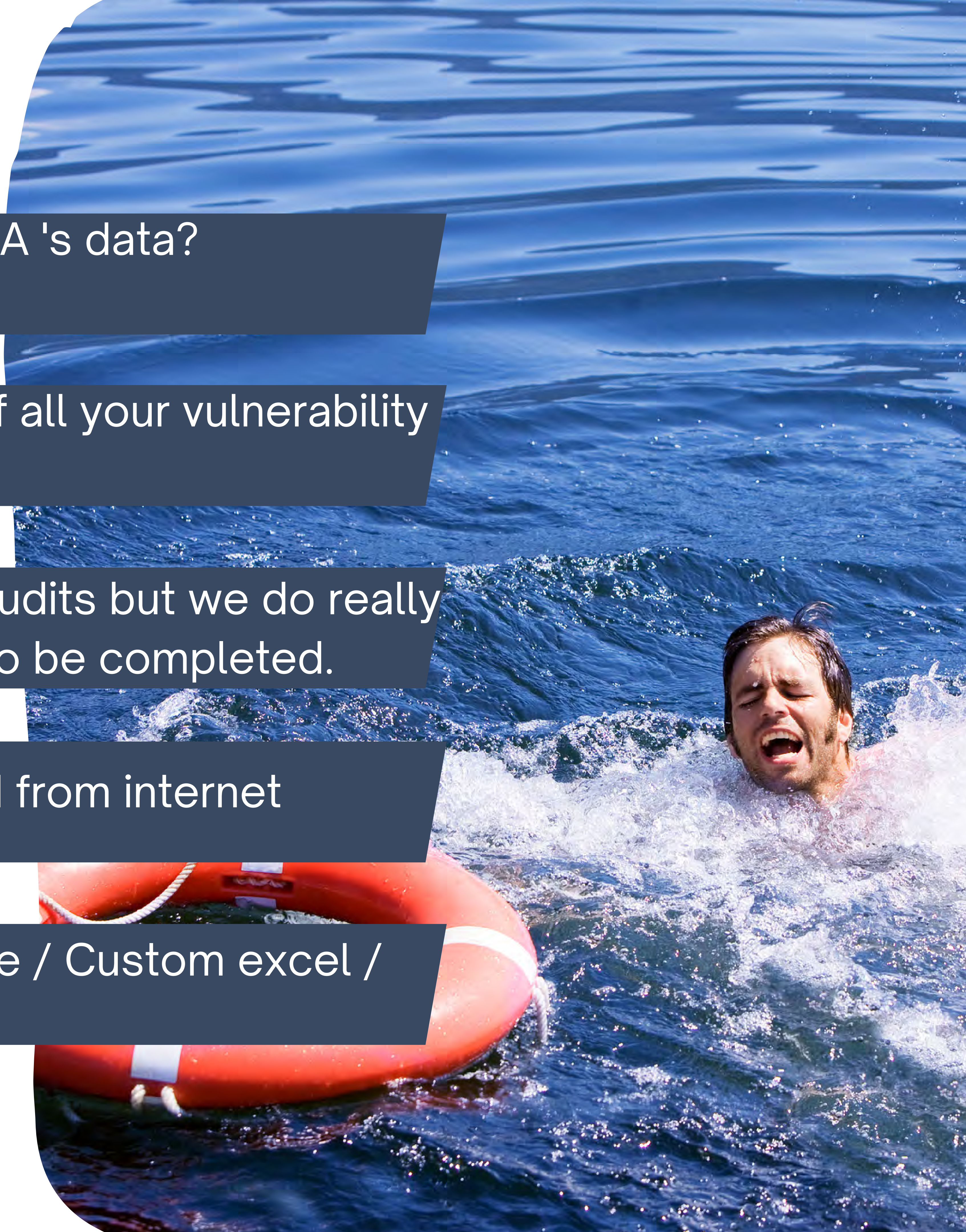
Thanks for the 5 external audits but we do really require this questionnaire to be completed.

Random

Questionnaire downloaded from internet

Inconsistent

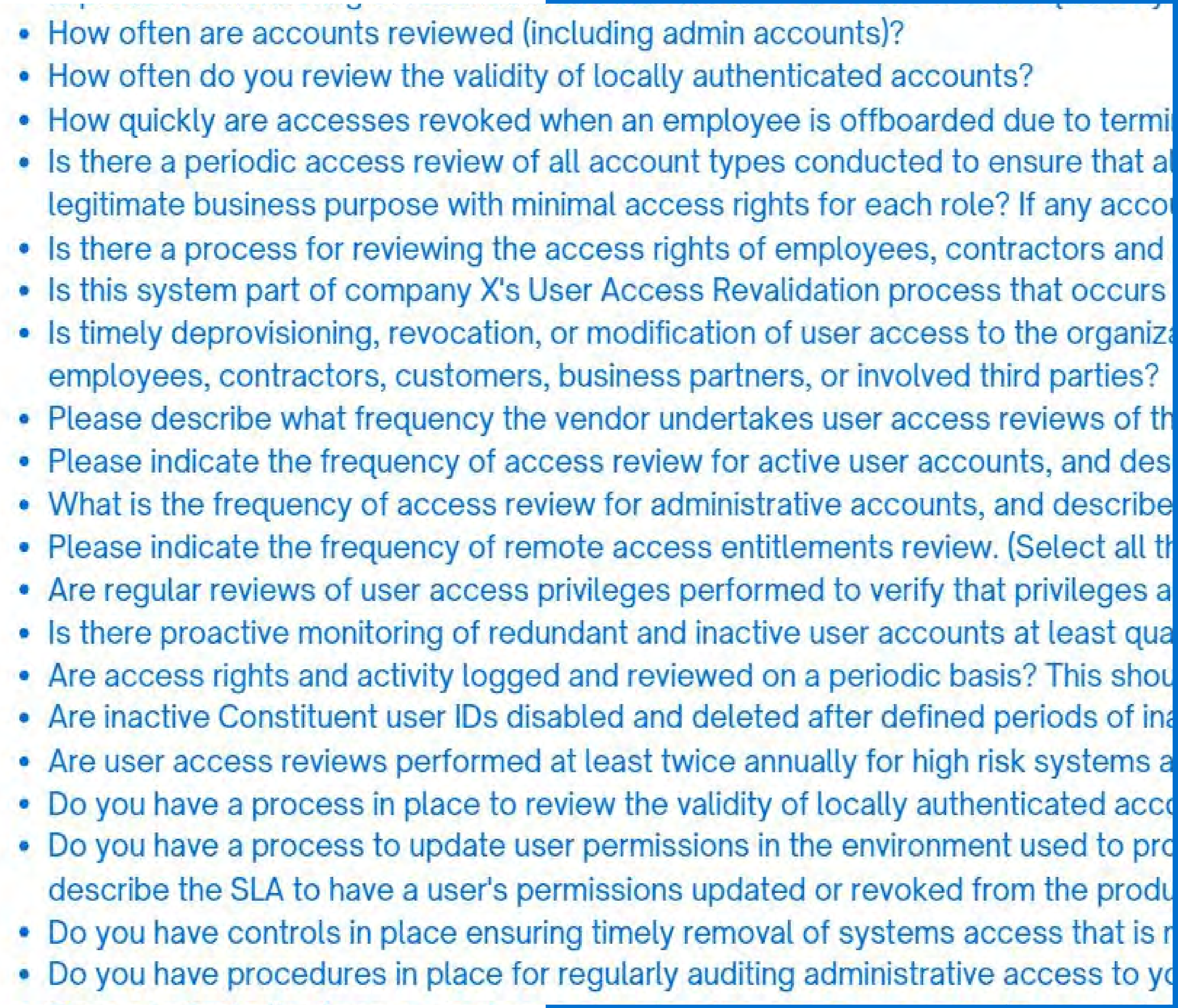
Word / Third party software / Custom excel / Emails



100 Ways to Ask the Same Question

How do you manage User Access Reviews?

- ☆ Frequency
- ☆ Standard vs Privileged
- ☆ Change in Roles
- ☆ Audit Trail



- How often are accounts reviewed (including admin accounts)?
- How often do you review the validity of locally authenticated accounts?
- How quickly are accesses revoked when an employee is offboarded due to termi
- Is there a periodic access review of all account types conducted to ensure that al legitimate business purpose with minimal access rights for each role? If any acco
- Is there a process for reviewing the access rights of employees, contractors and
- Is this system part of company X's User Access Revalidation process that occurs
- Is timely deprovisioning, revocation, or modification of user access to the organiza employees, contractors, customers, business partners, or involved third parties?
- Please describe what frequency the vendor undertakes user access reviews of th
- Please indicate the frequency of access review for active user accounts, and des
- What is the frequency of access review for administrative accounts, and describe
- Please indicate the frequency of remote access entitlements review. (Select all th
- Are regular reviews of user access privileges performed to verify that privileges a
- Is there proactive monitoring of redundant and inactive user accounts at least qua
- Are access rights and activity logged and reviewed on a periodic basis? This shou
- Are inactive Constituent user IDs disabled and deleted after defined periods of ina
- Are user access reviews performed at least twice annually for high risk systems a
- Do you have a process in place to review the validity of locally authenticated acco
- Do you have a process to update user permissions in the environment used to pro describe the SLA to have a user's permissions updated or revoked from the produ
- Do you have controls in place ensuring timely removal of systems access that is n
- Do you have procedures in place for regularly auditing administrative access to yo

Impacts to Companies from Security Questionnaires...

Requestor

Respondent

	🏢	🏛	🏬	🏪
🏢	😎	😎	🤔	🙄
🏛	😎	😎	🤔	🙄
🏬	😬	😬	🤔	🤔
🏪	😢	😢	😬	😬

Skills, Roles and Control Ownership

Do you encrypt all data that we provide you?

Sales

Product

IT

IT Security

Legal

Let's Do This...

- How do you secure your building?
- Is your network designed securely?
- Do you conduct user access reviews?
- What physical security controls do you have in place?
- Do you have a support team?
- How is access control managed?
- Do you have adequate survelliance in place?
- How do you manage incidents?

Our Response

Thank you for asking. Our company has a robust security program some of the features include:

- ✓ User Access Reviews are conducted annually and results documented.
- ✓ 24/7 support team.
- ✓ All equipment is appropriately labelled
- ✓ A well designed padlock and key function for additional security in highly secure working areas.
- ✓ Electronic keypads control every access point.
- ✓ Surveillance cameras are in place in every physical room.

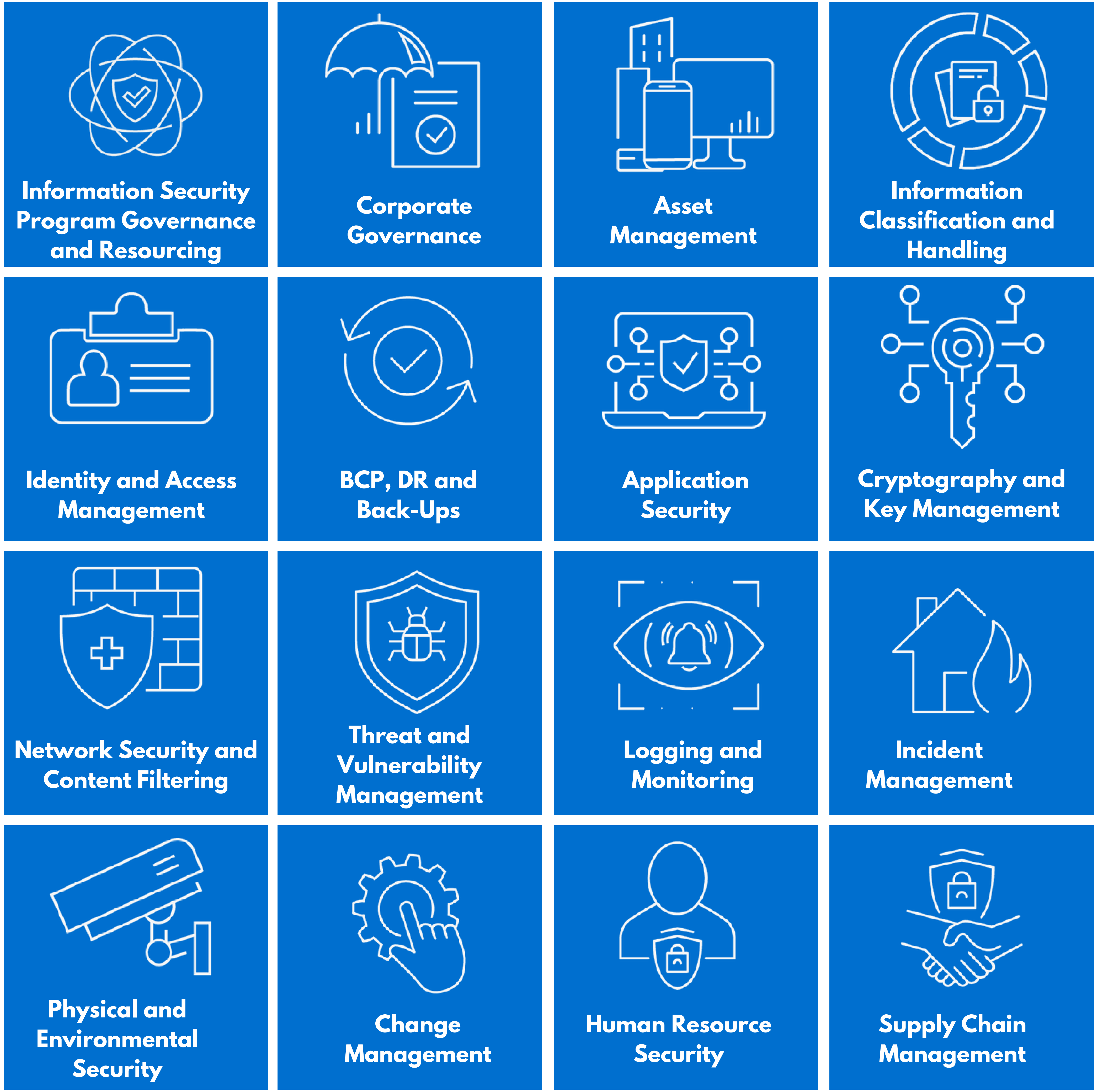
Upon Inspection.... 5 Years Later

Tips - If You Must...

INFOSECASSURE

How to respond	What to look for
Clarify scope if required such as naming the application or system that the response relates to.	Is the response specific to the services you use? Do they use shared security model? For which controls?
Use plain and complete language (no acronyms)	Do you understand the acronyms used?
Be clear even if the question doesn't ask for specific details.	If the answer is Yes or No, does this satisfy your question?
Be fair and accurate, if a control gap consult with control owner to identify compensating control	If response indicates a missing control are compensating controls described?
Collect information needed for traceability	Which controls should form part of regular reviews?
Provide documents or extract from documents where documents are protected, provide read-room access	If names of documents provided have you reviewed the atcual documents?

INFOSECASSURE



Information Security Program Governance and Resourcing

Corporate Governance

Asset Management

Information Classification and Handling

Identity and Access Management

BCP, DR and Back-Ups

Application Security

Cryptography and Key Management

Network Security and Content Filtering

Threat and Vulnerability Management

Logging and Monitoring

Incident Management

Physical and Environmental Security

Change Management

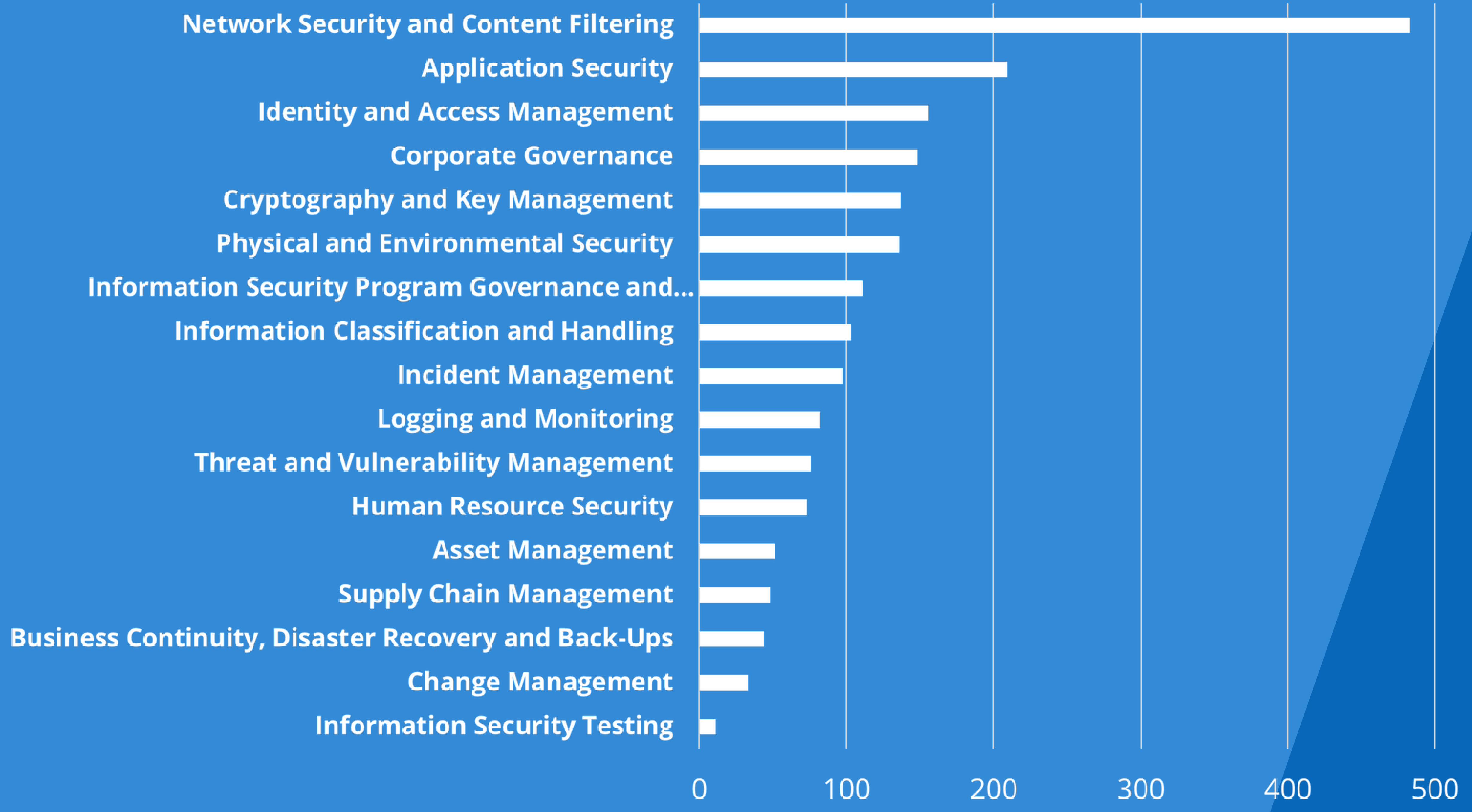
Human Resource Security

Supply Chain Management

Get it Right One Way - Let's Focus on Practice Areas

- Every control fits into this model
- Considers interactions with most business structures and team skills/functions
- Enables better management reporting
- Helps educate all

Many Frameworks, Many Controls, Many "Languages"



- PCI DSS
- OAIC Privacy Act
- Cloud Security Alliance
- APRA 234
- OWASP ASVS
- Aus Gov ISM
- Essential Eight Maturity Model
- 27001/17
- NIST CSF
- SOC 2

Wrap-Up

Know Your Supplier

Split the contract - Master and by Product/Service

Get Appropriate Agreements in Place

Reasonable and Regular Assurance

Manage Supplier Risks

Know Your Own Business

Standardise How You Assess Your Controls and Report to All

Build Assurance Preparation into your SDLC/PDLC

Take Aways

Sample Security Clauses

www.infosecassure.com.au/download/security-clauses

Practice Area Overview

www.infosecassure.com.au/download/infosecassure-practice-areas

Questionnaire Research Outcomes

www.infosecassure.com.au/download/questionnaire-research