Please note: This sample shows only a small part of the complete Gap Assessment tool.

ISO/IEC 27001 Gap Assessment Tool (Questionnaire Based)

ISMS-FORM-00-4

Terms used
ISMS: Information Security Management System

Information security management systems: Requirements

AREA/SECTION	SUB-SECTION	ISO/IEC 27001 REQUIREMENTS	REQS MET?	ACTION NEEDED TO MEET REQ	ACTION OWNER
4 Context of the organization					
4.1 Understanding the organization and its context		Have the external and internal issues that affect the ISMS been determined?	Yes		
4.2 Understanding the needs and expectations of interested parties		Have the interested parties and their requirements been identified?	Yes		
4.3 Determining the scope of the information security management system		Has the scope of the ISMS been determined and documented?	Yes		
4.4 Information security management system		Is an ISMS in place and being continually improved?	Yes		
		Totals:	**4**		
5 Leadership					
5.1 Leadership and commitment		Does top management demonstrate leadership and commitment to the ISMS by providing resources and communicating effectively? (see list A to	Yes		
5.2 Policy		Is a documented information security policy in place?	Yes		
		Does it set objectives for the ISMS?	Yes		
		Does it commit the organization to satsifying requirements and continually improving the ISMS?	Yes		
		Is it adequately communicated?	Yes		
5.3 Organizational roles, responsibilities and authorities		Are roles, responsibilities and authorities for the ISMS defined?	Yes		
		Totals:	**6**		

ISO/IEC 27017 Cloud Service Customer (CSC) Gap Assessment Tool (Questionnaire Based)

ISMS-FORM-00-4

Terms used
CSP = Cloud Service Provider
CSC = Cloud Service Customer

Code of practice for information security controls based on ISO/IEC 27002 for cloud services

Note: Only those controls that are listed in the ISO/IEC 27017 standard that apply to Cloud Service Customers (CSCs) are shown here.

AREA/SECTION	SUB-SECTION	ISO/IEC 27017 CSC REQUIREMENTS	REQS MET?	ACTION NEEDED TO MEET REQ	ACTION OWNER
A.5 Information security policies					
A.5.1 Management direction for information security	A.5.1.1 Policies for information security	Is there an information security policy for cloud computing?			
		Does the policy consider the specific risks associated with using cloud services?	Yes		
		Totals:	**2**		
A.6 Organization of information security					
A.6.1 Internal organization	A.6.1.1 Information security roles and responsibilities	Are the roles and responsibilities concerned with the security of the cloud service agreed between the CSC and the CSP and documented, including the interface with the CSP support function?			
	A.6.1.3 Contact with authorities	Are all of the authorities relevant to both the CSC and the CSP identified?	Yes		
CLD.6.3 Relationship between cloud service customer and cloud service provider	CLD.6.3.1 Shared roles and responsibilities within a cloud computing environment	Are cloud service users aware of their roles and responsibilities in using each cloud service?			
		Totals:	**3**		
A.7 Human resources security					
A.7.2 During employment	A.7.2.2 Information security awareness, education and training	Do awareness training efforts include the specific risks and issues to do with the use of cloud services?			
		Totals:	**1**		
A.8 Asset management					
A.8.1 Responsibility for assets	A.8.1.1 Inventory of assets	Are information assets stored in the cloud included on the asset inventory?	Yes		
	CLD.8.1.5 Removal of cloud service customer assets	When terminating a cloud service, is the process clear and documented and does it cover all of the assets involved?	Yes		
A.8.2 Information classification	A.8.2.2 Labelling of information	Are assets stored in the cloud appropriately labelled?			
		Totals:	**3**		

ISO/IEC 27017 Cloud Service Provider (CSP) Gap Assessment Tool (Questionnaire Based)

ISMS-FORM-00-4

Terms used
CSP = Cloud Service Provider
CSC = Cloud Service Customer

Code of practice for information security controls based on ISO/IEC 27002 for cloud services

Note: Only those controls that are listed in the ISO/IEC 27017 standard that apply to Cloud Service Providers (CSPs) are shown here.

AREA/SECTION	SUB-SECTION	ISO/IEC 27017 CSP REQUIREMENTS	REQS MET?	ACTION NEEDED TO MEET REQ	ACTION OWNER
A.5 Information security policies					
A.5.1 Management direction for information security	A.5.1.1 Policies for information security	Has the information security policy been augmented to reflect the specific risks associated with operating as a cloud service provider?	Yes		
		Totals:	**1**		
A.6 Organization of information security					
A.6.1 Internal organization	A.6.1.1 Information security roles and responsibilities	Have information security responsibilities been defined between parties in the cloud relationship?	Yes		
	A.6.1.3 Contact with authorities	Have customers been informed of the geographical spread of the CSP's operations and the countries involved?	Yes		
CLD.6.3 Relationship between cloud service customer and cloud service provider	CLD.6.3.1 Shared roles and responsibilities within a cloud computing environment	Has the split of responsibilities for information security been documented and made clear to customers?	Yes		
		Totals:	**3**		
A.7 Human resources security					
A.7.2 During employment	A.7.2.2 Information security awareness, education and training	Do awareness training efforts include the specifi risks and issues to do with the use of cloud services?	Yes		
		Totals:	**1**		
A.8 Asset management					
A.8.1 Responsibility for assets	A.8.1.1 Inventory of assets	Is a distinction made between cloud service customer data and cloud service derived data?	Yes		
	CLD.8.1.5 Removal of cloud service customer assets	Is information provided to customers regarding procedures used for the removal of a customer service and associated data?	Yes		
A.8.2 Information classification	A.8.2.2 Labelling of information	Have facilities that are provided for the customer to label their data been communicated to the customer?	Yes		
		Totals:	**3**		

ISO/IEC 27018 Gap Assessment Tool (Questionnaire Based)

ISMS-FORM-00-4

Terms used

CSP = Cloud Service Provider
CSC = Cloud Service Customer
PII = Personally Identifiable Information

Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

Note: Only those controls that are listed in the ISO/IEC 27018 standard are shown here.

AREA/SECTION	SUB-SECTION	ISO/IEC 27017 CSP REQUIREMENTS	REQS MET?	ACTION NEEDED TO MEET REQ	ACTION OWNER
A.5 Information security policies					
A.5.1 Management direction for information security	A.5.1.1 Policies for information security	Does the CSP information security policy include a statement committing to meeting PII protection legislation and contractual terms?	Yes		
		Are information security responsibilities between CSP, sub-contractors and CSC clearly allocated in contractual agreements?	Yes		
		Totals:	**2**		
A.6 Organization of information security					
A.6.1 Internal organization	A.6.1.1 Information security roles and responsibilities	Is a CSP point of contact identified for CSCs regarding PII processing?	Yes		
		Totals:	**1**		
A.7 Human resources security					
A.7.2 During employment	A.7.2.2 Information security awareness, education and training	Are CSP employees made aware of the importance of protecting PII and the consequences of failing to do so?	Yes		
		Totals:	**1**		
A.8 Asset management					
		Totals:	**0**		
A.9 Access control					
A.9.2 User access management	A.9.2.1 User registration and de-registration	Do procedures address the situation where user access has been compromised e.g. stolen passwords?	Yes		
	A.9.4.2 Secure log-on procedures	Are secure log-on procedures available if requested by the CSC?	Yes		
		Totals:	**2**		

Please note: This sample shows only a small part of the Gap Assessment results.

Gap assessment results

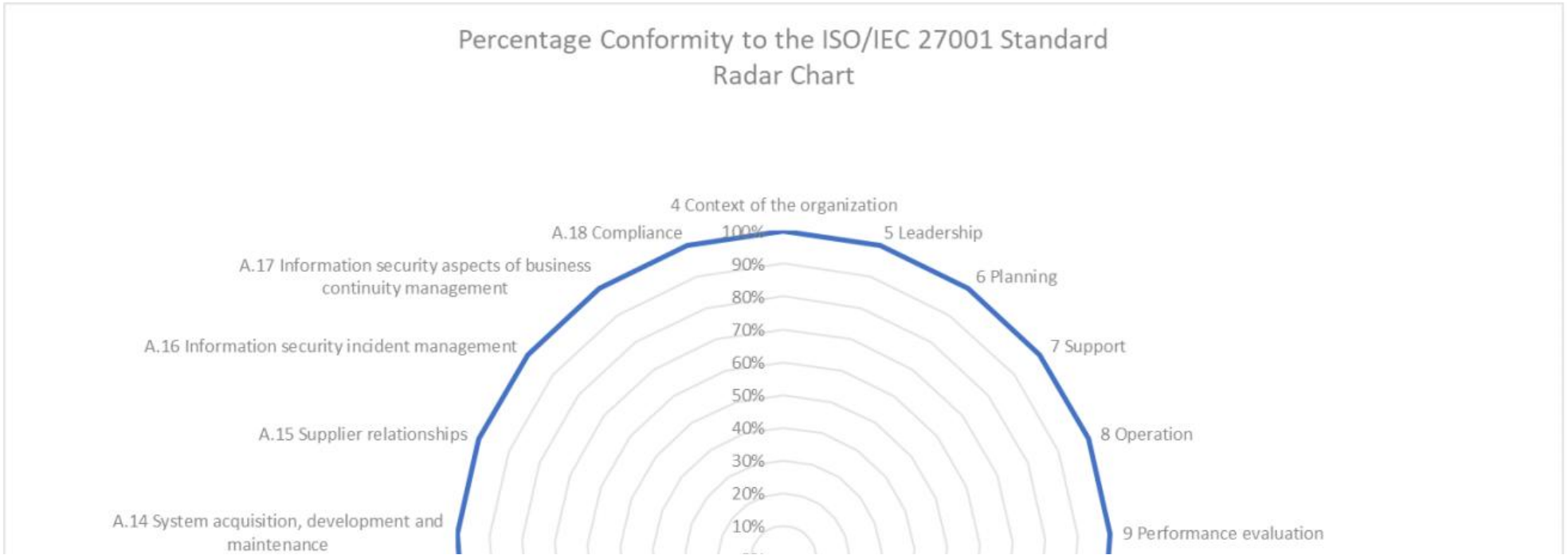
ISO/IEC 27001 Information Security Standard

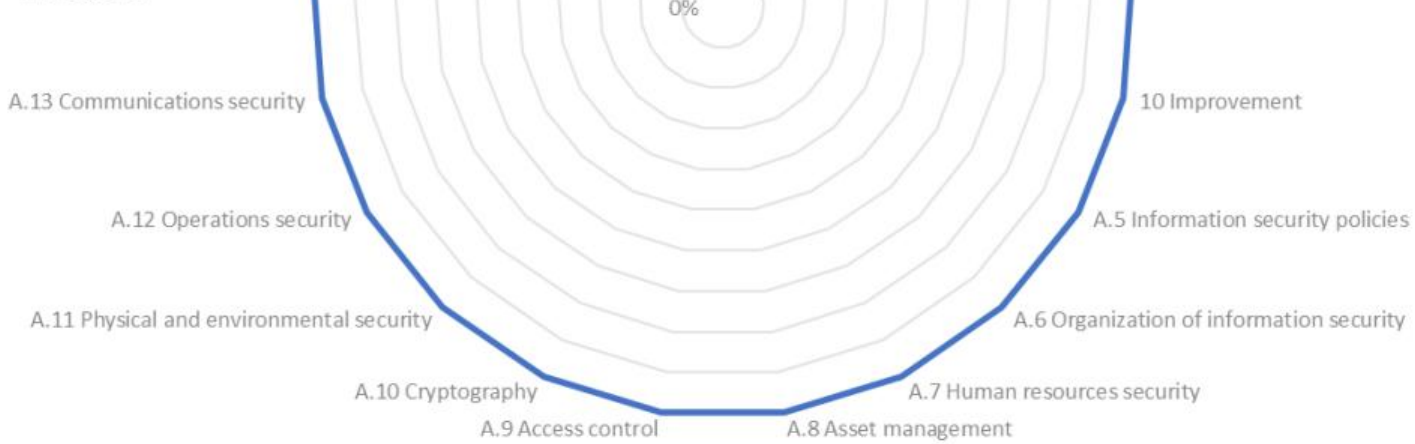
AREA OF STANDARD	REQS IN SECTION	NO OF REQS MET	PERCENTAGE CONFORMANT
4 Context of the organization	4	4	100%
5 Leadership	6	6	100%
6 Planning	16	16	100%
7 Support	8	8	100%
8 Operation	4	4	100%
9 Performance evaluation	6	6	100%
10 Improvement	2	2	100%
A.5 Information security policies	2	2	100%
A.6 Organization of information security	7	7	100%
A.7 Human resources security	6	6	100%
A.8 Asset management	10	10	100%
A.9 Access control	14	14	100%
A.10 Cryptography	2	2	100%
A.11 Physical and environmental security	15	15	100%
A.12 Operations security	14	14	100%
A.13 Communications security	7	7	100%
A.14 System acquisition, development and maintenance	13	13	100%
A.15 Supplier relationships	5	5	100%
A.16 Information security incident management	7	7	100%
A.17 Information security aspects of business continuity management	4	4	100%
A.18 Compliance	8	8	100%
Totals	**160**	**160**	**100%**

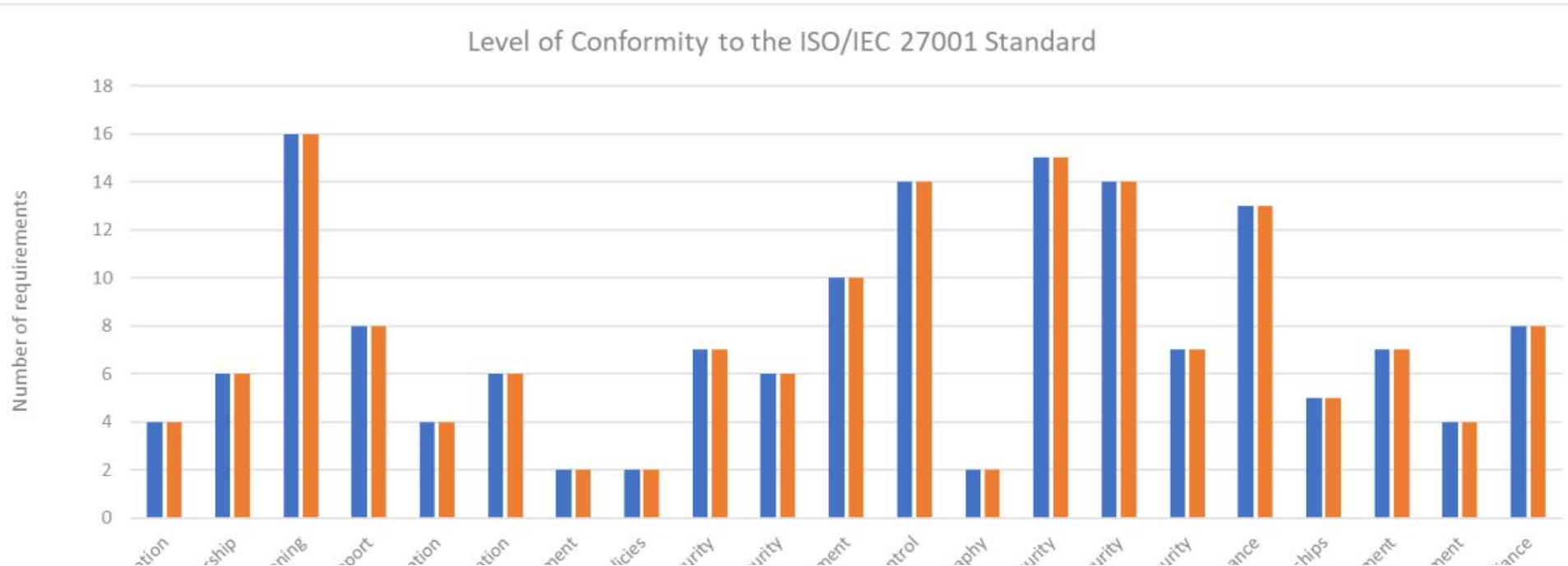
ISO/IEC 27017 Code of Practice for Cloud Services: Cloud Service Customer (CSC)

AREA OF CODE OF PRACTICE	REQS IN SECTION	NO OF REQS MET	PERCENTAGE CONFORMANT
A.5 Information security policies	2	2	100%
A.6 Organization of information security	3	3	100%
A.7 Human resources security	1	1	100%
A.8 Asset management	3	3	100%
A.9 Access control	6	6	100%
A.10 Cryptography	2	2	100%

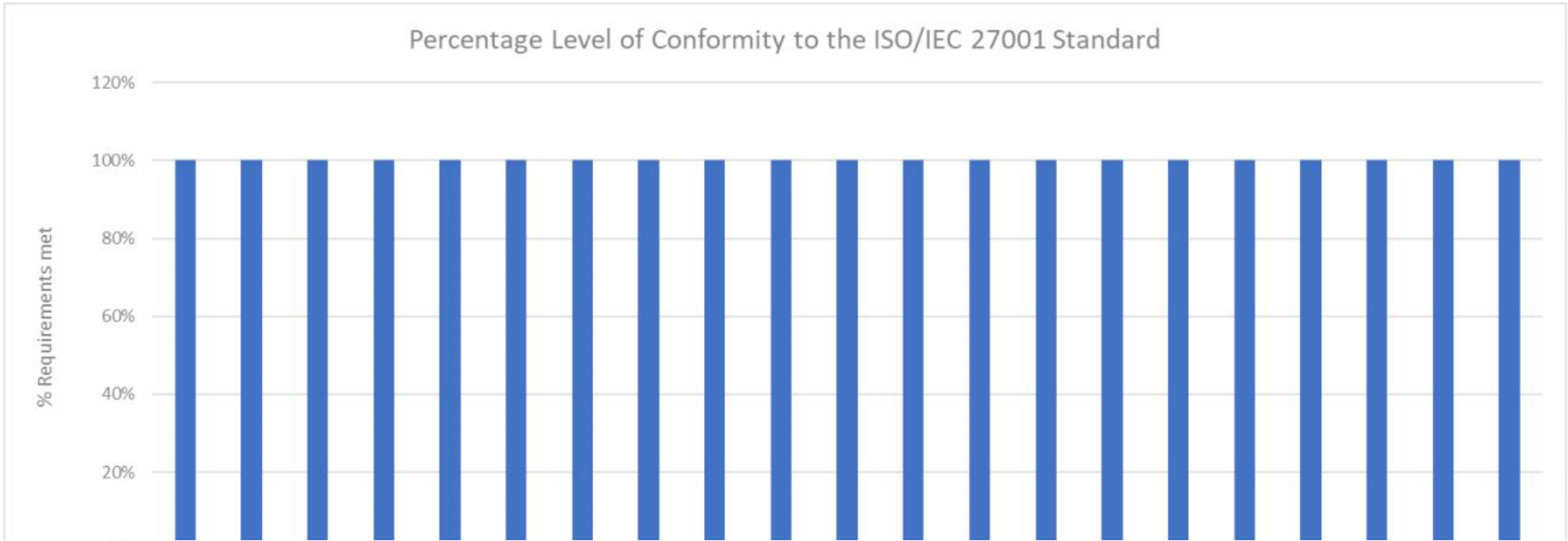
A.11 Physical and environmental security		1	1	100%
A.12 Operations security		9	9	100%
A.13 Communications security		1	1	100%
A.14 System acquisition, development and maintenance		2	2	100%
A.15 Supplier relationships		2	2	100%
A.16 Information security incident management		3	3	100%
A.17 Information security aspects of business continuity management		0	0	100%
A.18 Compliance		5	5	100%
	Totals	**40**	**40**	**100%**

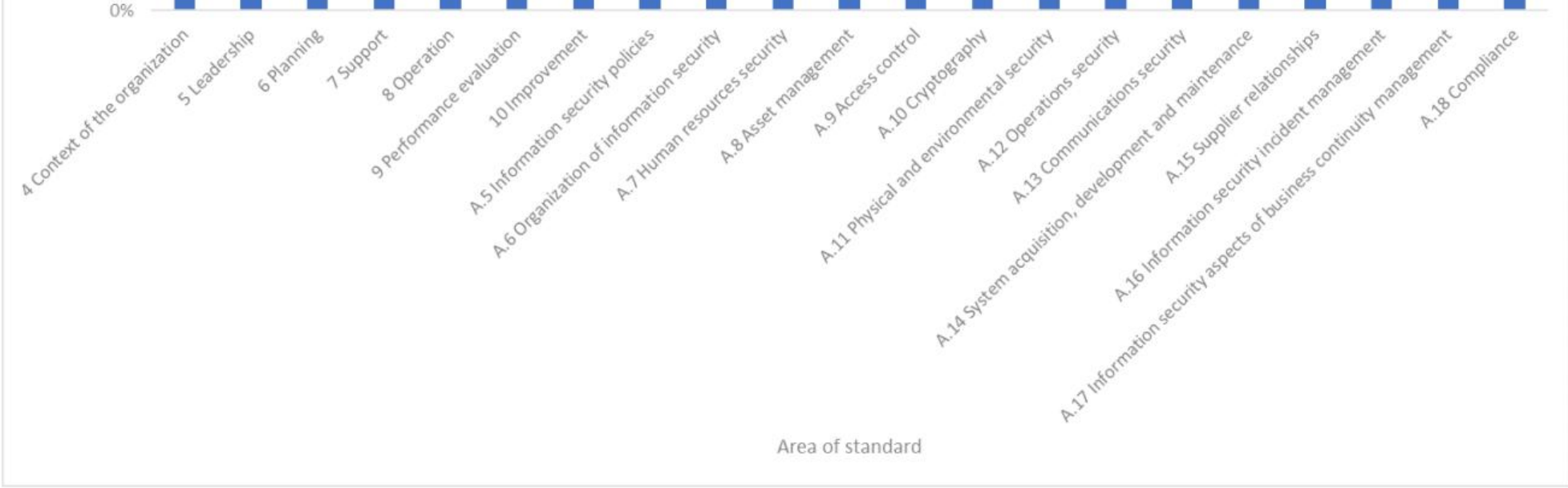


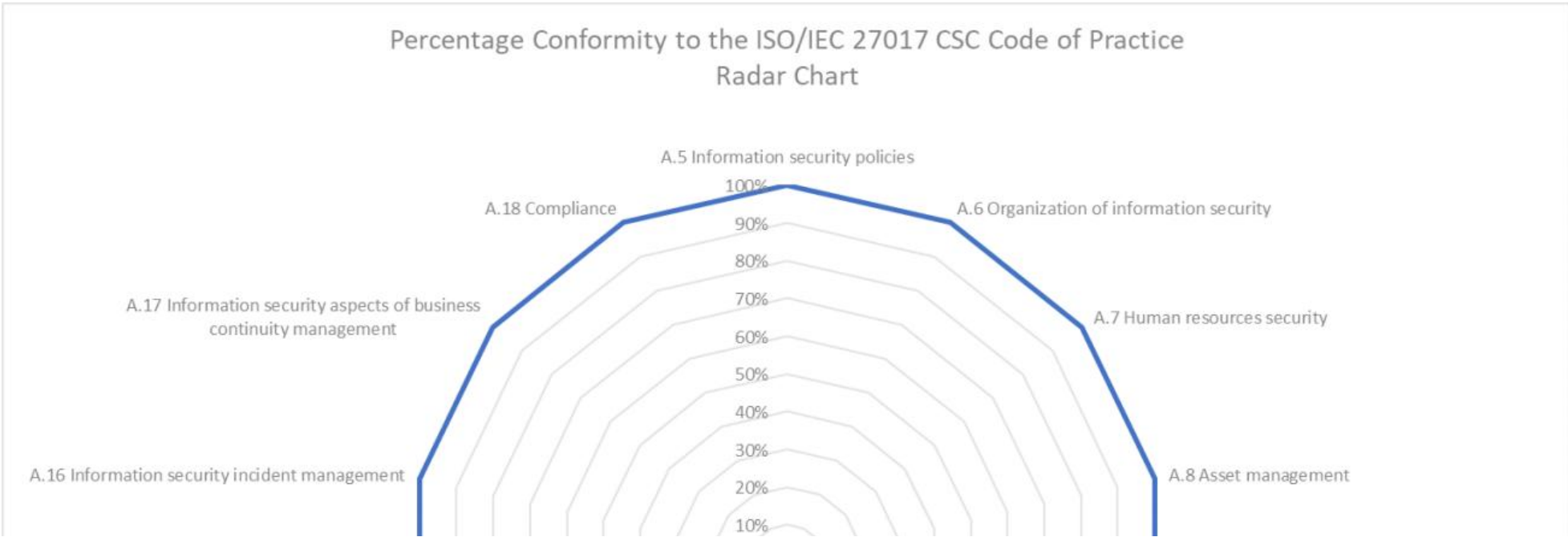

0%
10 Improvement
A.5 Information security policies
A.6 Organization of information security
A.7 Human resources security
A.8 Asset management
A.9 Access control
A.10 Cryptography
A.11 Physical and environmental security
A.12 Operations security
A.13 Communications security

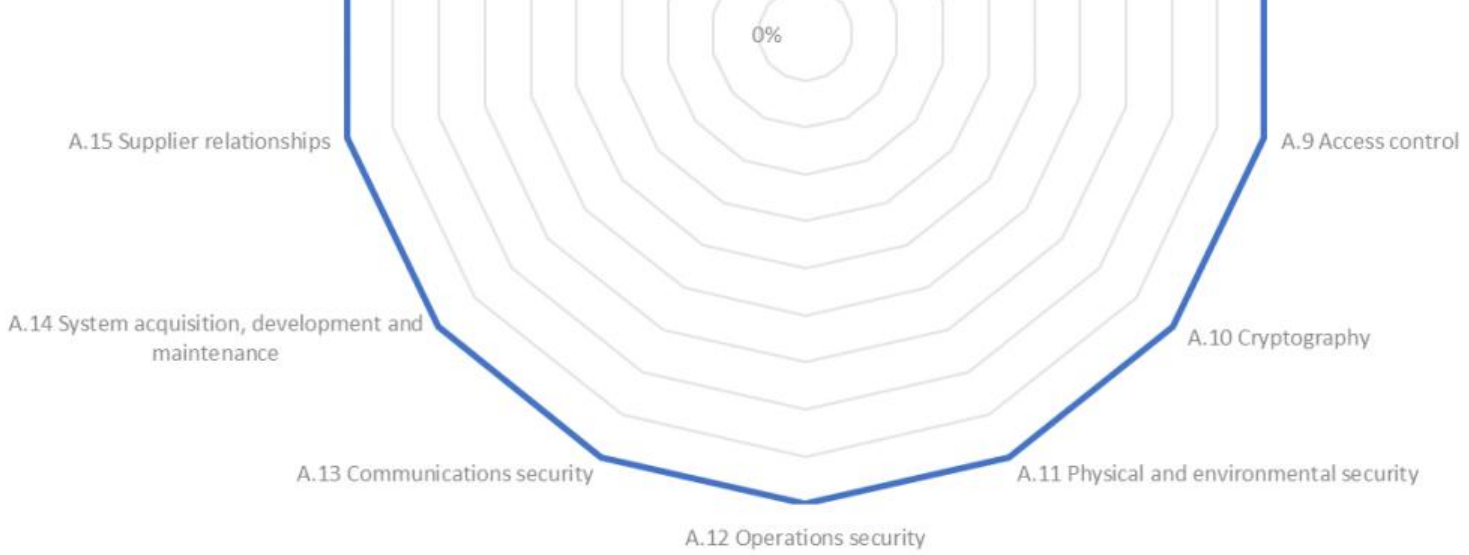

Level of Conformity to the ISO/IEC 27001 Standard
Number of requirements
18
16
14
12
10
8
6
4
2
0

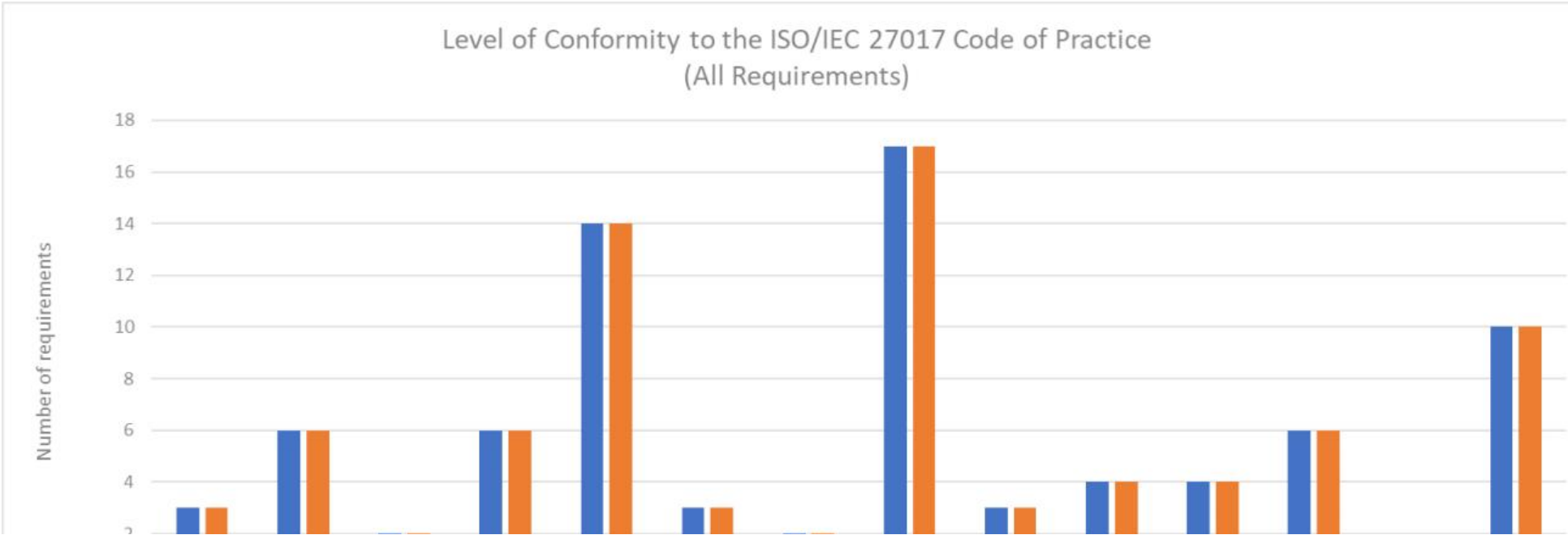

4 Context of the organiza
5 Leader
6 Plan
7 Supp
8 Opera
9 Performance evalua
10 Improven
A.5 Information security po
A.6 Organization of information sec
A.7 Human resources sec
A.8 Asset manage
A.9 Access co
A.10 Cryptogra
A.11 Physical and environmental sec
A.12 Operations sec
A.13 Communications sec
A.14 System acquisition, development and maintena
A.15 Supplier relations
A.16 Information security incident manage
A.17 Information security aspects of business continuity manage
A.18 Compli
Area of standard
REQS IN SECTION
NO OF REQS MET

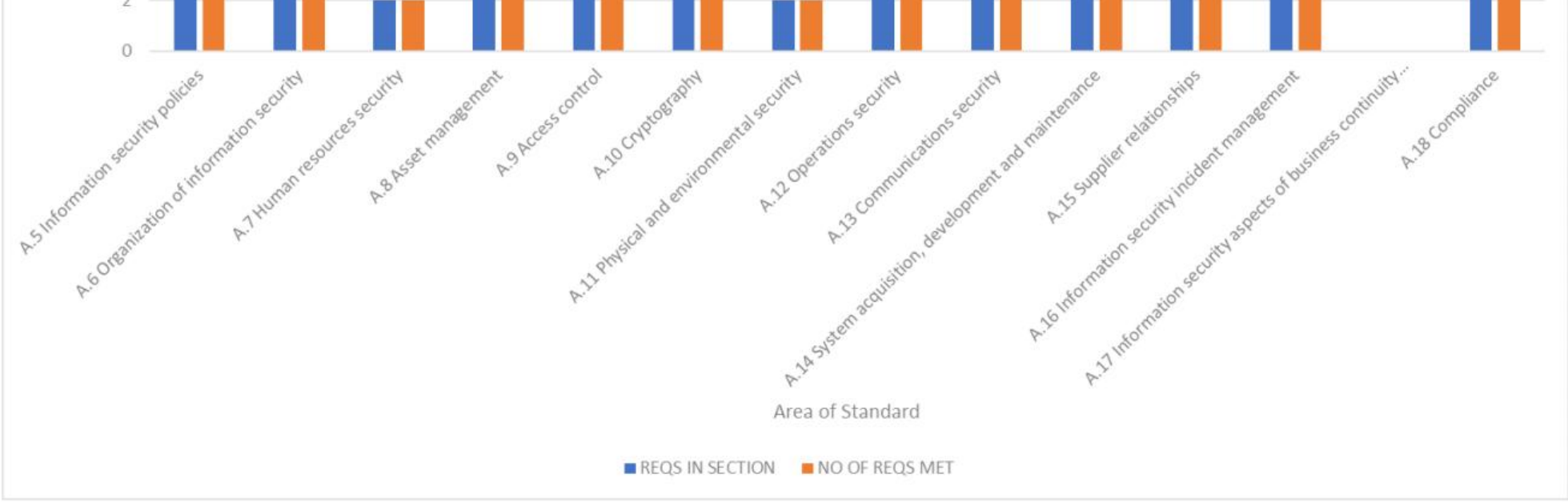

Percentage Level of Conformity to the ISO/IEC 27001 Standard
120%
100%
80%
60%
40%
20%
% Requirements met

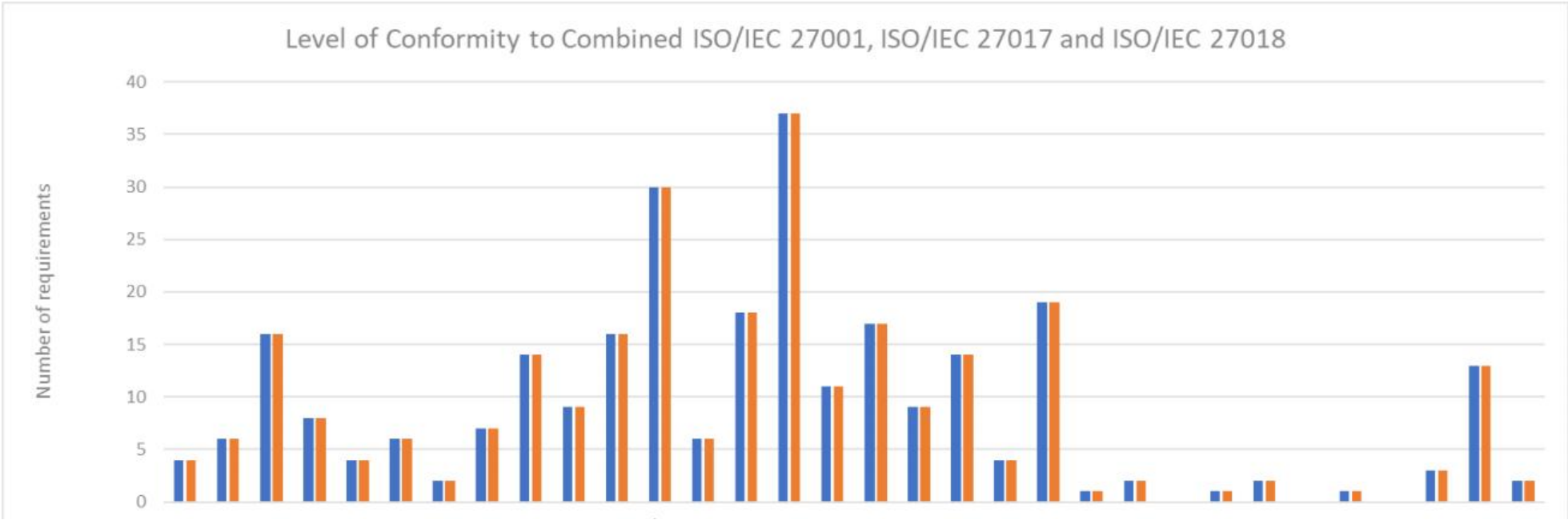

0%
4 Context of the organization
5 Leadership
6 Planning
7 Support
8 Operation
9 Performance evaluation
10 Improvement
A.5 Information security policies
A.6 Organization of information security
A.7 Human resources security
A.8 Asset management
A.9 Access control
A.10 Cryptography
A.11 Physical and environmental 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
Area of standard


Percentage Conformity to the ISO/IEC 27017 CSC Code of Practice
Radar Chart
A.5 Information security policies
A.6 Organization of information security
A.7 Human resources 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
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%


0%
A.15 Supplier relationships
A.9 Access control
A.14 System acquisition, development and maintenance
A.10 Cryptography
A.13 Communications security
A.11 Physical and environmental security
A.12 Operations security


Level of Conformity to the ISO/IEC 27017 Code of Practice
(All Requirements)
Number of requirements
18
16
14
12
10
8
6
4


0
A.5 Information security policies
A.6 Organization of information security
A.7 Human resources 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...
A.18 Compliance
Area of Standard
REQS IN SECTION
NO OF REQS MET


Level of Conformity to Combined ISO/IEC 27001, ISO/IEC 27017 and ISO/IEC 27018
Number of requirements
40
35
30
25
20
15
10
5
0


4 Context of the organization
5 Leadership
6 Planning
7 Support
8 Operation
9 Performance evaluation
10 Improvement
A.5 Information security policies
A.6 Organization of information security
A.7 Human resources 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
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
Area of Standard
REQS IN SECTION
NO OF REQS MET