



**Statement of applicability.** Translation from 'Verklaring van toepasselijkheid Bio-ITech BV Versie 2.0 24/08/2016'

Clause	Reasons for controls selection					
	LR	CO	BR/BP	RRA	AP	IMP
<b>Security Policies</b>						
5.1.1				x	YES	YES
5.1.2				x	YES	YES
<b>Organisation of information security</b>						
6.1.1				x	YES	YES
6.1.2				x	YES	YES
6.1.3	x			x	YES	YES
6.1.4				x	YES	YES
6.1.5				x	YES	YES
6.2.1				x	YES	YES
6.2.2				x	YES	YES
<b>Human resource security</b>						
7.1.1				x	YES	YES
7.1.2				x	YES	YES
7.2.1				x	YES	YES
7.2.2				x	YES	YES
7.2.3				x	YES	YES
7.3.1				x	YES	YES
<b>Asset management</b>						
8.1.1				x	YES	YES
8.1.2				x	YES	YES
8.1.3				x	YES	YES
8.1.4				x	YES	YES
8.2.1				x	YES	YES
8.2.2				x	YES	YES
8.2.3				x	YES	YES
8.3.1				x	YES	YES
8.3.2				x	YES	YES
8.3.3				x	YES	YES
<b>Access control</b>						
9.1.1				x	YES	YES
9.1.2				x	YES	YES
9.2.1				x	YES	YES
9.2.2				x	YES	YES
9.2.3				x	YES	YES
9.2.4				x	YES	YES
9.2.5				x	YES	YES
9.2.6				x	YES	YES
9.3.1				x	YES	YES
9.4.1				x	YES	YES
9.4.2				x	YES	YES
9.4.3			x	x	YES	YES
9.4.4				x	YES	YES
9.4.5				x	YES	YES
<b>Cryptography</b>						
10.1.1				x	YES	YES
10.1.2				x	YES	YES



Physical and environmental security				
11.1.1	Physical security perimeter	x	YES	YES
11.1.2	Physical entry controls	x	YES	YES
11.1.3	Securing office, room and facilities	x	YES	YES
11.1.4	Protecting against external and environmental threats	x	YES	YES
11.1.5	Working in secure areas	x	YES	YES
11.1.6	Delivery and loading areas	x	YES	YES
11.2.1	Equipment siting and protection	x	YES	YES
11.2.2	Supporting utilities	x	YES	YES
11.2.3	Cabling security	x	YES	YES
11.2.4	Equipment maintenance	x	YES	YES
11.2.5	Removal of assets	x	YES	YES
11.2.6	Security of equipment and assets off-premises	x	YES	YES
11.2.7	Secure disposal or re-use of equipment	x	YES	YES
11.2.8	Unattended user equipment	x	YES	YES
11.2.9	Clear desk and clear screen policy	x	YES	YES
Operations security				
12.1.1	Documented operating procedures	x	YES	YES
12.1.2	Change management	x	YES	YES
12.1.3	Capacity management	x	YES	YES
12.1.4	Separation of development, testing and operational environments	x	YES	YES
12.2.1	Controls against malware	x	YES	YES
12.3.1	Information backup	x	YES	YES
12.4.1	Event logging	x	YES	YES
12.4.2	Protection of log information	x	YES	YES
12.4.3	Administrator and operator logs	x	YES	YES
12.4.4	Clock synchronisation	x	YES	YES
12.5.1	Installation of software on operational systems	x	YES	YES
12.6.1	Management of technical vulnerabilities	x	YES	YES
12.6.2	Restrictions on software installation	x	YES	YES
12.7.1	Information systems audit controls	x	YES	YES
Communications security				
13.1.1	Network controls	x	YES	YES
13.1.2	Security of network services	x	YES	YES
13.1.3	Segregation in networks	x	YES	YES
13.2.1	Information transfer policies and procedures	x	YES	YES
13.2.2	Agreements on information transfer	x	YES	YES
13.2.3	Electronic messaging	x	YES	YES
13.2.4	Confidentiality or non-disclosure agreements	x	YES	YES
System acquisition, development and maintenance				
14.1.1	Information security requirements analysis and specification	x	YES	YES
14.1.2	Securing applications services on public networks	x	YES	YES
14.1.3	Protecting application services transactions	x	YES	YES
14.2.1	Secure development policy	x	YES	YES
14.2.2	System change control procedures	x	YES	YES
14.2.3	Technical review of applications after operating platform changes	x	YES	YES
14.2.4	Restrictions on changes to software packages	x	YES	YES
14.2.5	Secure system engineering principles	x	YES	YES
14.2.6	Secure development environment	x	YES	YES
14.2.7	Outsourced development	x	YES	YES



14.2.8	System security testing		x	YES	YES
14.2.9	System acceptance testing		x	YES	YES
14.3.1	Protection of test data		x	YES	YES
<b>Supplier relationships</b>					
15.1.1	Information security policy for supplier relationships		x	YES	YES
15.1.2	Addressing security within supplier agreements		x	YES	YES
15.1.3	Information and communication technology supply chain		x	YES	YES
15.2.1	Monitoring and review of supplier services		x	YES	YES
15.2.2	Managing changes to supplier services		x	YES	YES
<b>Information security incident management</b>					
16.1.1	Responsibilities and procedures		x	YES	YES
16.1.2	Reporting information security events		x	YES	YES
16.1.3	Reporting information security weaknesses		x	YES	YES
16.1.4	Assessment of and decision on information security events		x	YES	YES
16.1.5	Response to information security incidents		x	YES	YES
16.1.6	Learning from information security incidents		x	YES	YES
16.1.7	Collection of evidence	x	x	YES	YES
<b>Information security aspects of business continuity management</b>					
17.1.1	Planning information security continuity		x	YES	YES
17.1.2	Implementing information security continuity		x	YES	YES
17.1.3	Verify, review and evaluate information security continuity		x	YES	PARTLY
17.2.1	Availability of information processing facilities	x	x	YES	YES
<b>Compliance</b>					
18.1.1	Identification of applicable legislation and contractual requirements	x	x	YES	YES
18.1.2	Intellectual property rights		x	YES	YES
18.1.3	Protection of records		x	YES	YES
18.1.4	Privacy and protection of personally identifiable information	x	x	YES	YES
18.1.5	Regulation of cryptographic controls		x	YES	YES
18.2.1	Independent review of information security		x	YES	YES
18.2.2	Compliance with security policies and standards		x	YES	YES
18.2.3	Technical compliance review		x	YES	YES
LR	legal requirements				
CO	contractual obligations				
BR/BP	business requirements/adopted best practices				
RRA	results of risk assessment				
AP	applicable				
AMP	implemented				