

A conceptual Guide to:

Enterprise Information Security

2023

By, Tommy Babel, Co-Founder & CEO
www.cyzea.io

Contents

7	Introduction
9	Information Security
9	Digital Transformation
10	Cyber Security
10	Cyber Security Awareness
11	Crown Jewels
11	Data Protection
12	Private Information
13	CIA Model
13	Layers-of-defense
14	Defense in-depth
15	Assume Breach
17	NIST
17	NIST CSF
18	NIST SP800-53
19	ISO/IEC 2700x
20	ISMS
21	ISO/IEC 27001
23	GRC
23	Cyber Risks
24	Risk Management
25	Cyber Risk Assessment
26	Information Security Controls
26	NIST SP800-171
28	Controls Maturity
29	CMMC
31	TPRM
31	Cloud transformation
32	Outsourcing Security
33	Vendor Lock
35	Situational Awareness
35	Attack Surface

36	Cyber Threats
37	Social Engineering
37	Spear-Phishing
38	BEC
38	MALWARE
39	Lateral Movement
40	Privilege Escalation
40	RCE
41	APT
41	NIST Threat Modeling
42	MITRE
43	MITRE T2
44	MITRE Att@ck
45	Red Team
46	Blue Team
46	Purple Team
47	Penetration Testing
48	Blackbox, Graybox, Whitebox
50	Enterprise Network
50	Enterprise Architecture
51	Enterprise Security
52	Perimeter Security
52	DMZ
53	Network CLASS
54	The OSA model
55	UDP vs TCP
55	Network Security
56	SSL Decryption
57	DNS Security
57	SPF/DMARC
58	Anti-DDOS
59	Firewall
59	IDS / IPS

60	NAC
60	Network Segmentation
61	Micro Segmentation
62	Secure Remote Access
62	MPLS
63	VPN
63	Site to Site VPN
64	IPSEC
65	MFA
65	Zero-Trust Access
66	SDN
66	SD-WAN
67	SDP
69	Endpoint Security
69	Secure Internet Access
70	SWG
70	SEG
71	Sandboxing
72	EDR
72	Application Control
73	Vulnerability Management
73	Risk based Vulnerability Management
74	Virtual Patching
76	Identity and Access Governance (IAG)
76	RBAC
77	Least Privilege
78	Application Accounts
79	PAM
79	Secure Active Directory
81	Password Management Policy
81	NIST SP800-63B
82	IAM
83	SOD

83	SOX
84	Service Organization Control
86	Application Security
86	SOA
87	SOA alternatives
88	Microservices
88	Event driven Architecture
89	S-SDLC
90	Risk Assessment
90	Threat Modeling
91	OWASP TOP-10
92	SANS Top-25
93	Secure Code Analysis
93	SAST
94	DAST
94	Change Management
95	Secure Deployment
96	Application Testing
96	Sprint Coding
98	QA security testing
98	Product Security
99	Secure Key and Secret Management
100	Secure Data Handling
100	Secure Code Repositories
101	WAF
102	API Gateway
102	SBOM
105	Data Protection
105	Database Security
106	Dynamic data masking and static data masking
107	File System Security & Challenges
108	UEBA
109	DRM