	Organisational	People/*Physical*	Technical
High Priority	▪ ACCESS CONTROL (Passwords, MFA) ▪ SUPPLIER SECURITY	▪ EMPLOYEE SCREENING ▪ SECURITY AWARENESS TRAINING ▪ *PERIMETER AND ENTRY*	▪ ANTI-MALWARE ON DEVICES ▪ CLOUD CONFIGURATION ▪ PATCHING AND UPDATES
Level 2	▪ DATA DISCOVERY ▪ PRIVILEGED ACCESS MANAGEMENT ▪ SOFTWARE SUPPLY CHAIN/OPEN SOURCE RISK ▪ LEGAL, REGULATORY, CONTRACTUAL	▪ EMPLOYMENT CONTRACTS ▪ CONFIDENTIALITY/NDA ▪ *MONITORING OF PHYSICAL RISKS*	▪ BACKUPS ▪ CRYPTOGRAPHY
Level 3	▪ INFOSEC POLICY ▪ THREAT INTEL ▪ CHANGE MANAGEMENT ▪ ALLOCATION AND RETURN OF ASSETS ▪ CLASSIFICATION AND MANAGEMENT OF SENSITIVE DATA ▪ SDLC ▪ INCIDENT MANAGEMENT ▪ BUSINESS CONTINUITY/ ▪ DISASTER RECOVERY ▪ OPERATING PROCEDURES ▪ REMOTE WORKING ▪ ACCEPTABLE USE ▪ VULN DISCLOSURE		▪ LOGGING AND MONITORING ▪ DLP ▪ WAF ▪ IDENTITY MANAGEMENT ▪ VULNERABILITY SCANNING ▪ PENETRATION TESTING
Level 4 (Frameworks)	▪ ISO27001, SOC2, PCI DSS etc…		

Prioritisation of information security technical measures and procedures

Kiowa
INFORMATION SECURITY