INFORMATION SECURITY CONTROLS

PREVENTIVE

🟪 Information Security Policies 🛠 📄 P01	🟦 Secure Network Architecture 📄 🛠 P05	🟦 Data Classification 📄 🛠 P09	🟦 Firewalls 🛠 P13	🟦 Anti-Malware Protection (AV) 🛠 P17	🟦 Email Security Gateway 🛠 P21	🟦 Endpoint Protection (EDR/NGAV) 🛠 P25	🟦 Vulnerability Management 🛠 P29	🟦 Database Hardening 🛠 P33	🟦 API Security Hardening P37	🟩 Application Security SAST/DAST P41	🟩 Encryption in Transit P45
🟪 Risk Assessment & Treatment 📄 P02	🟦 Network Segmentation 📄 🛠 P06	🟦 Secure Cloud Configuration 📄 🛠 P10	🟦 Configuration Management 🛠 P14	🟦 Identity & Access Management 🛠 P18	🟦 Web Application Firewall (WAF) 🛠 P22	🟦 Privileged Account Management 🛠 P26	🟦 Secure Boot & Firmware Integrity 🛠 P30	🟦 Device Encryption 🛠 P34	🟦 USB/ Removable Media Controls P38	🟩 Change Management P42	🟨 Physical Access Control (BADGES, BIOMETRICS) P46
🟪 Security Awareness & Training 📄 P03	🟦 Zero Trust (ZTNA) 📄 🛠 P07	🟦 Container & Orchestration Security 📄 🛠 P11	🟦 Patch Management 🛠 P15	🟦 Mobile Device Management 🛠 P19	🟦 Secure Remote Access (VPN, etc) 🛠 P23	🟦 Data Loss Prevention (DLP) 🛠 P27	🟦 Secure Admin Workstations 🛠 P31	🟦 Application Sandboxing 🛠 P35	🟩 Principle of Least Privilege P39	🟩 Email DMARC SPF/DKIM Enforcement P43	🟨 Secure Areas P47
🟪 Third Party Risk Management 📄 P04	🟦 Secure SDLC 📄 P08	🟦 Security Awareness Trainings 📄 P12	🟦 MFA / User Authentication 🛠 P16	🟦 Intrusion Prevention System (IPS) 🛠 P20	🟦 Application Whitelisting 🛠 P24	🟦 Backup Encryption & Immutability 🛠 P28	🟦 Web Content Filtering 🛠 P32	🟦 Privileged Session Recording 🛠 P36	🟩 Wireless Security P40	🟩 Web Application Security P44	🟨 Media Sanitisation & Disposal P48

DETECTIVE

🟦 SIEM 🛠 D01	🟦 End-Point Detection (EDR/XDR) 🛠 D05	🟦 DNS Filtering Logging & Analysis 🛠 D09	🟦 Threat Intelligence Platform (TIP) 🛠 D13	🟦 Cloud Security Posture Management D17	🟪 External Audit D21	🟪 Change Management Audit Logs D25	🟪 Backup Verification & Testing D29	🟪 Security Awareness Reporting D33	🟨 Physical Intrusion Detection D37	🟩 Penetration Testing D41	🟩 Social Media Monitoring D45
🟦 Intrusion Detection System (IDS) 🛠 D02	🟦 Antivirus & Malware Detection 🛠 D06	🟦 Cloud Audit Logs D10	🟦 SSL/TLS Inspection & Decryption 🛠 D14	🟦 Web Proxy Filtering & Logging 🛠 D18	🟪 Policy Exception Review D22	🟪 Third-Party Risk Assessment D26	🟪 Table-top Exercises (BCP/DR) D30	🟪 Exit Interviews D34	🟨 Physical Inventory Checks D38	🟩 Regular Vulnerability Scans D42	🟩 Red Team Exercises D46
🟦 Vulnerability Management System (VMS) 🛠 D03	🟦 Data Loss Prevention (DLP) 🛠 D07	🟦 Database Activity Monitoring (DAM) 🛠 D11	🟦 Email Gateway Security Logging 🛠 D15	🟦 Honeypot & Decoys 🛠 D19	🟪 User Access Review D23	🟪 Code Reviews D27	🟪 Security Metrics D31	🟪 Risk Register Review D35	🟨 Environmental Alarm Monitoring D39	🟩 Phishing Simulation Campaign D43	🟩 Security Incident Detection D47
🟦 File Integrity Monitoring (FIM) 🛠 D04	🟦 User Behaviour Analytics (UEBA) 🛠 D08	🟦 Network Traffic Analysis (NTA) 🛠 D12	🟦 Breach & Attack Simulation (BAS) 🛠 D16	🟪 Internal Audit D20	🟪 Privileged Accounts Monitoring D24	🟪 Data Classification Audit D28	🟪 Job Rotation & Mandatory Vacation D32	🟨 Video Surveillance (CCTV) D36	🟨 Visitor Log Review D40	🟩 Dark Web Monitoring D44	🟩 Canary Tokens Honeytokens D48

CORRECTIVE

🟦 AV/Malware Remediation 🛠 C01	🟦 DB Recovery (Rollback etc) C05	🟦 Update IPS/IDS Signatures C09	🟦 Reconfigure Firewall C13	🟪 Root Cause Analysis (RCA) C17	🟪 Risk Register Update C21	🟪 Authorisation Revocation C25	🟨 Visitor Log Review C29	🟨 Secure Compromised Server Rooms C33	🟩 Forensic Investigation C37	🟩 Secure Code Remediation C41	🟩 Red-Teaming Follow up C45
🟦 Patch Deployment (Post Incident) C02	🟦 Remove Malicious User Account C06	🟦 Sandbox Analysis / Cleanup C10	🟦 Deploy Compensating Controls C14	🟪 Update Vendor Contracts C18	🟪 Lessons Learned (Post-Mortem) C22	🟨 Replace Faulty Equipment C26	🟨 Restoration of Power Systems (UPS) C30	🟩 Incident Response Procedures C34	🟩 Containment & Eradication C38	🟩 Change Rollback C42	🟩 Block IPs / Indicators of Compromise C46
🟦 EDR Remediation 🛠 C03	🟦 Apply Hotfixes C07	🟦 System Re-imaging C11	🟦 Endpoint Isolation & Reintegration C15	🟪 User Retraining C19	🟪 Audit Finding Remediation C23	🟨 Reposition Security Cameras C27	🟨 Replace Tampered Media C31	🟩 Disaster Recovery Procedures C35	🟩 Hardening Configuration C39	🟩 Rotate Credentials C43	🟩 Terminate Sessions C47
🟦 Restoration from Backup 🛠 C04	🟦 Revoke Compromised Certificates C08	🟦 IaC Recovery C12	🟪 Update Security Policies C16	🟪 Disciplinary Action C20	🟪 Post-Incident Compliance Reporting C24	🟨 Access Badge Deactivation C28	🟨 Reset Alarm Systems C32	🟩 Business Continuity Plan Execution C36	🟩 User Communication C40	🟩 Update SOC Playbooks C44	🟩 Tune SIEM Alerts C48

+j

🟪 administrative 🟦 technical 🟨 physical 🟩 operational 📄 design principles 🛠 technological measures

This compilation of controls is drawn from ISO/IEC 27001:2022, NIST SP 800-53 Rev. 5, and CIS Controls v8. It is not intended to be an exhaustive list. Some controls have been consolidated into broader categories, while others—such as those pertaining to OT and AI—have been omitted. Controls can also be grouped as administrative, technological, operational, and physical; in practice, many span multiple categories. For example, data classification is an administrative control but typically depends on technological solutions for effective execution and lifecycle management; change management is both a preventive and a detective control, whereas patch management can be both preventive and corrective. Network segmentation is an architectural control, but its enforcement relies on technical configuration and deployment tools.

CONCEPT & DESIGN AHMED ANWAR
forebrook
forebrook.com/resources