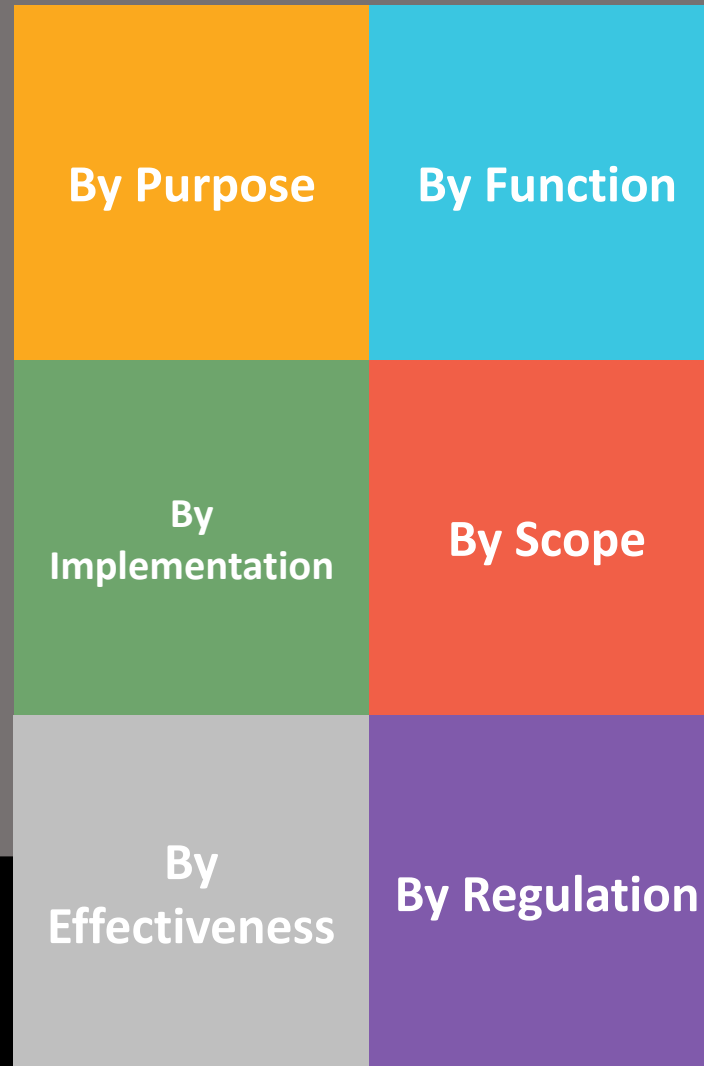


# Classification Of Cybersecurity Controls /Definitions/

**Directive controls** are designed to instruct, guide, and mandate certain activities and behavior. **Deterrent controls** are deployed to discourage the violation of a security function. **Preventive controls** are proactive in that they attempt to deter or prevent risk realization. **Detective controls** are designed to detect and identify security incidents or anomalies. **Corrective controls** are responds to incidents or anomalies. **Recovery controls** provide the means to respond to a security breach and fix an issue.

**Automated controls** are performed entirely by a computer system. **Manual controls** are performed by individuals interacting with another individual or a system. **Hybrid controls** involve human intervention in a computer system, but the person's action is dependent on the wanted output from a system.

**Primary controls** are the main measures on which an organization relies to mitigate risks to digital assets to an acceptable level. **Secondary controls** help improve on effectiveness of primary controls but are not essential to the overall security posture.



**Administrative controls** are non-technical measures focused on managing people and control workplace risks. **Technical controls** use technology to remediate vulnerabilities or counteract threats in computer system. **Physical controls** are the set of measures taken to protect digital assets from physical threats that could harm, damage, or disrupt operations of computer systems.

**Application controls** are the safeguards designed to provide reasonable assurance that objectives relevant to a given application are achieved. **General controls** ensure the proper development, implementation and operation of applications and the integrity of data and computer operations.

**Privacy controls** are safeguards employed to ensure system compliance with applicable privacy requirements and manage privacy risks. **Fraud controls** deter fraud and keep an organization in compliance with the law. **Safety controls** aim at reducing life and health hazard risks from the use of computer systems. **Quality controls** are focused on the maintainance of products and services quality. **Defense controls** protect military industry support information a government creates or possesses, or that an entity creates or possesses for or on behalf of a government.



# Classification Of Cybersecurity Controls /Examples/

## By Purpose

**Directive:** *data retention plan*

**Deterrent:** *job rotation, warnings*

**Preventive:** *access control, IPS*

**Detective:** *honeypot, SOAR*

**Corrective:** *CSIRP, patching*

**Recovery:** *backup restore, failover*

## By Function

**Administrative:** *policy, SoD, data classification, metrics*

**Technical:** *firewall, antivirus, MFA, PKI, IDS, SIEM*

**Physical:** *fences, gates, locks, CCTV, badges, sensors*

## By Implementation

**Automated:** *PKI, EDR, IAM, IDP/IPS, ASCA, ACL, attack simulation*

**Manual:** *SOP, RACI matrix, reviews, reports, sign-offs, reconciliations*

**Hybrid:** *batch job, assisted workflow, semi-automated response*

## By Scope

**General:** *incident response, security awareness, logging*

**Application:** *data entry validation, authentication, authorization, permissions, exception reports*

## By Effectiveness

**Primary:** *media marking, vetting, application whitelisting*

**Secondary/Compensating:** *dual authorization, predictive maintenance, dynamic reconfiguration*

## By Regulation

**Privacy:** *masking, purging*

**Quality:** *lessons learned*

**Fraud:** *reconciliation, limits*

**Defense:** *classification*

**Safety:** *redundancy, fail-safe defaults*



Naiden  
Nedelchev © 2024

