Exam Objectives that do NOT Exist in Security+ SY0-401 but ARE in SY0-501

OBJ/Sub-OBJ	NEW in 501
5.0 Risk Management	
5.1 Explain the importance of policies, plans and procedures related to organizational security.	
· System administrator	NEW
· System owner	NEW
· User	NEW
· Privileged user	NEW
· Executive user	NEW
o Continuing education	NEW
o Adverse actions	NEW
· General security policies	
o Personal email	NEW
5.2 Summarize business impact analysis concepts.	
· Mission-essential functions	NEW
o Life	NEW
o Property	NEW
o Safety	NEW
o Finance	NEW
o Reputation	NEW
· Privacy impact assessment	NEW
· Privacy threshold assessment	NEW
5.3 Explain risk management processes and concepts.	
· Threat assessment	
o Environmental	NEW
o Manmade	NEW
o Internal vs. external	NEW
· Risk assessment	
o Asset value	NEW
o Risk register	NEW
o Supply chain assessment	
5.4 Given a scenario, follow incident response procedures.	
· Incident response plan	
o Cyber-incident response teams	NEW
5.5 Summarize basic concepts of forensics.	
· Legal hold	NEW

· Preservation	NEW
5.6 Explain disaster recovery and continuity of operation concepts.	
· Order of restoration	NEW
· Geographic considerations	
o Off-site backups	NEW
o Distance	NEW
o Location selection	NEW
o Legal implications	NEW
o Data sovereignty	NEW
· Continuity of operation planning	
o Failover	NEW
5.7 Compare and contrast various types of controls.	
· Physical	NEW
5.8 Given a scenario, carry out data security and privacy practices.	
· Data destruction and media sanitization	
o Burning	NEW
o Shredding	NEW
o Pulping	NEW
o Pulverizing	NEW
o Degaussing	NEW
o Purging	NEW
· Data sensitivity labeling and handling	
o PII	NEW
o PHI	NEW
· Data roles	
o Owner	NEW
o Steward/custodian	NEW
o Privacy officer	NEW
· Change management	
5.4 Given a scenario, follow incident response procedures.	
· Incident response plan	
o Documented incident types/category definitions	
o Roles and responsibilities	
o Reporting requirements/escalation	
o Cyber-incident response teams	NEW
o Exercise	
· Incident response process	
o Preparation	
o Identification	
o Containment	
o Eradication	
o Recovery	
o Lessons learned	

5.5 Summarize basic concepts of forensics.	
· Order of volatility	
· Chain of custody	
· Legal hold	NEW
· Data acquisition	
o Capture system image	
o Network traffic and logs	
o Capture video	
o Record time offset	
o Take hashes	
o Screenshots	
o Witness interviews	
· Preservation	NEW
· Recovery	
5.6 Explain disaster recovery and continuity of operation concepts.	
· Recovery sites	
· Order of restoration	NEW
· Geographic considerations	
o Off-site backups	NEW
o Distance	NEW
o Location selection	NEW
o Legal implications	NEW
o Data sovereignty	NEW
· Continuity of operation planning	
o Failover	NEW
5.7 Compare and contrast various types of controls.	
· Physical	NEW
5.8 Given a scenario, carry out data security and privacy practices.	
· Data destruction and media sanitization	
o Burning	NEW
o Shredding	NEW
o Pulping	NEW
o Pulverizing	NEW
o Degaussing	NEW
o Purging	NEW
· Data sensitivity labeling and handling	
o PII	NEW
o PHI	NEW
· Data roles	
o Owner	NEW
o Steward/custodian	NEW
o Privacy officer	NEW