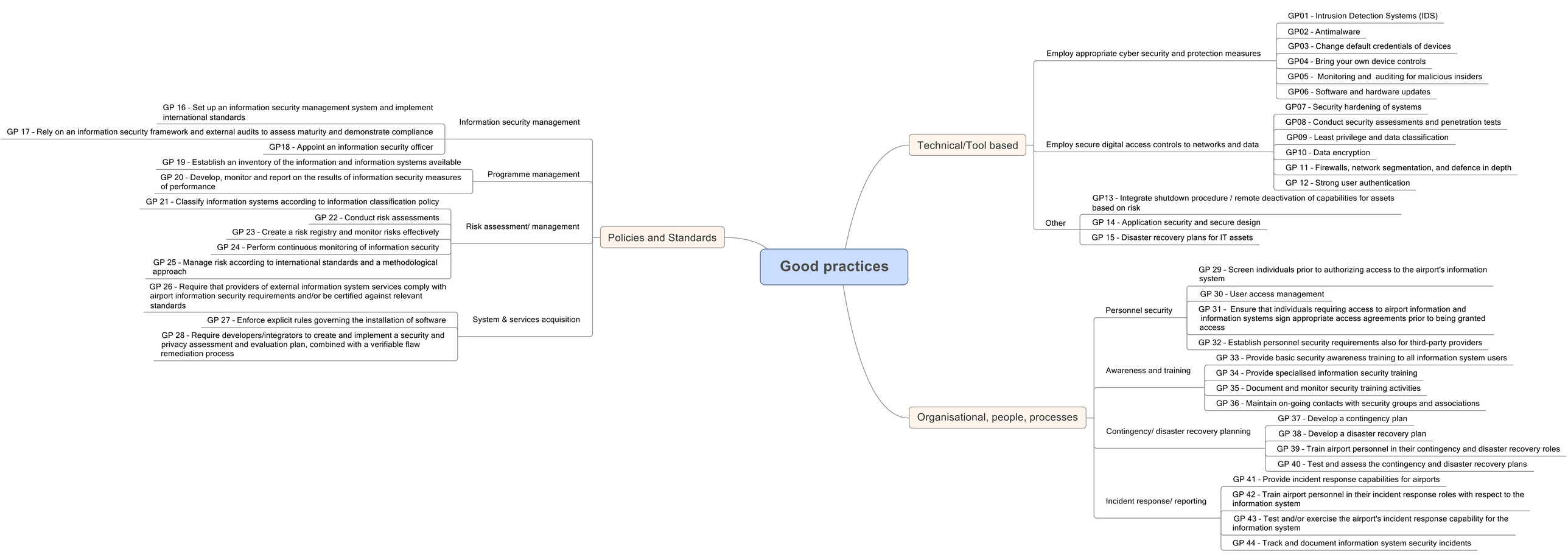
Good practices
Policies and Standards
Information security management
GP 16 - Set up an information security management system and implement international standards
GP 17 - Rely on an information security framework and external audits to assess maturity and demonstrate compliance
GP18 - Appoint an information security officer
Programme management
GP 19 - Establish an inventory of the information and information systems available
GP 20 - Develop, monitor and report on the results of information security measures of performance
Risk assessment/ management
GP 21 - Classify information systems according to information classification policy
GP 22 - Conduct risk assessments
GP 23 - Create a risk registry and monitor risks effectively
GP 24 - Perform continuous monitoring of information security
GP 25 - Manage risk according to international standards and a methodological approach
System & services acquisition
GP 26 - Require that providers of external information system services comply with airport information security requirements and/or be certified against relevant standards
GP 27 - Enforce explicit rules governing the installation of software
GP 28 - Require developers/integrators to create and implement a security and privacy assessment and evaluation plan, combined with a verifiable flaw remediation process
Technical/Tool based
Employ appropriate cyber security and protection measures
GP01 - Intrusion Detection Systems (IDS)
GP02 - Antimalware
GP03 - Change default credentials of devices
GP04 - Bring your own device controls
GP05 - Monitoring and auditing for malicious insiders
GP06 - Software and hardware updates
Employ secure digital access controls to networks and data
GP07 - Security hardening of systems
GP08 - Conduct security assessments and penetration tests
GP09 - Least privilege and data classification
GP10 - Data encryption
GP 11 - Firewalls, network segmentation, and defence in depth
GP 12 - Strong user authentication
Other
GP13 - Integrate shutdown procedure / remote deactivation of capabilities for assets based on risk
GP 14 - Application security and secure design
GP 15 - Disaster recovery plans for IT assets
Organisational, people, processes
Personnel security
GP 29 - Screen individuals prior to authorizing access to the airport's information system
GP 30 - User access management
GP 31 - Ensure that individuals requiring access to airport information and information systems sign appropriate access agreements prior to being granted access
GP 32 - Establish personnel security requirements also for third-party providers
Awareness and training
GP 33 - Provide basic security awareness training to all information system users
GP 34 - Provide specialised information security training
GP 35 - Document and monitor security training activities
GP 36 - Maintain on-going contacts with security groups and associations
Contingency/ disaster recovery planning
GP 37 - Develop a contingency plan
GP 38 - Develop a disaster recovery plan
GP 39 - Train airport personnel in their contingency and disaster recovery roles
GP 40 - Test and assess the contingency and disaster recovery plans
Incident response/ reporting
GP 41 - Provide incident response capabilities for airports
GP 42 - Train airport personnel in their incident response roles with respect to the information system
GP 43 - Test and/or exercise the airport's incident response capability for the information system
GP 44 - Track and document information system security incidents