infopulse

Levels of Enterprise Security_

Domains	Levels of Enterprise Security				
	Entry	**Basic**	**Challengers**	**Mature**	**Highly Secure**
People	○ No dedicated security personnel or overlapping responsibilities ○ Outdated security qualifications or skills ○ Lack of security awareness	○ Part-time or shared security personnel ○ Some vendor training sessions conducted ○ Basic security education for non-IT personnel	○ Defined CISO functions ○ Ongoing security awareness training sessions ○ Security team is not fully staffed ○ Regular vendor training sessions conducted	○ Security teams are extended with third-party services ○ Defined common security roles ○ Highly skilled and educated security teams	○ Red/Blue teaming with internal teams conducted ○ Bug-bounty program in place ○ Extensive security budget
Process	○ All security activities occur ad-hoc ○ Reactive approach to security management ○ No strategic or mid-term security management plans	○ Clear communications flow between the IT and security teams ○ Security responsibility segregation is defined to a certain extent ○ Various security processes defined and documented ○ Security roles assigned across the organization	○ Defined security strategy ○ Corporate assets labeled and categorized ○ Well-documented IT infrastructure ○ Security responsibility segregation is clearly defined ○ Measured and controlled security process metrics	○ High coverage of security processes ○ Regular security assessments ○ Process-driven IT and security management approach ○ KPIs for all major IT and security processes in place ○ Obtained security certifications ○ Secure-by-design approach	○ Proactive approach to security management ○ Cooperation with third-party security teams or governmental bodies ○ Direct communications with vendors concerning the improvements of security solutions ○ RBAC and Least privilege approach implemented ○ Security best practices implemented and regularly reviewed

Domains	Levels of Enterprise Security				
	Entry	**Basic**	**Challengers**	**Mature**	**Highly Secure**
Technology	○ No IT infrastructure standardization ○ Absence of centralized management ○ Lack of security visibility	○ Certain security systems in place ○ Security solutions not fine-tuned ○ Several infrastructure components are managed centrally ○ Insufficient security visibility	○ Relevant security solutions in place ○ Centralized management of key security solutions and IT assets ○ Full security visibility over business-critical assets ○ Advanced security solutions used ○ Security solutions are updated to the latest versions and patches	○ Security risk assessment solutions and technologies implemented ○ Security solutions regularly fine-tuned with respect to the changing cyber landscape ○ Regular validation of security controls ○ Automated upgrades to the latest versions and patches ○ Custom security solutions in use	○ Enterprise-wide automation of security operations ○ Implementation of next-gen security solutions ○ Threat intelligence deployed ○ Complete security visibility ○ Multi-layered and multi-vendor security approach