Confidentiality محرمانه بودن – عدم دسترسي شخص ثالث غير مجاز، به اطلاعات پيغام دادهاي تنها توسط فرستنده و گيرنده قابل مشاهده باشد

Identification شناسايي – حصول اطمينان از هويت كاربر مقابل

Authentication تشخيص هويت - تائيد صلاحيت – تائيد احراز ارسال پيام از همان منبع مورد ادعا گيرنده پيغام، هويت فرستنده را شناسايي كند.

Non – Repudiation

عدم رد يا انكار – بين داده پيام و مرجع آن رابطه غير غابل انكار وجود داشته باشد تا ارسال كننده پس از ارسال و دريافت كننده پس از دريافت قادر به رد يا انكار آن نباشند .

Integrity تماميت – صحت- اصمينان از اينكه پيام دريافت شده همان چيزي است كه ارسال شده پيغام دادهاي را تنها فرستنده ميتواند بدون اين كه تشخيص داده شود تغيير دهد

Public Key كليد عمومي – رمزي كه به همكاران جهت ارسال نامه محرمانه داده مي شود

Private Key كليد خصوصي – رمز خاص كاربر كه هيچكس از آن مطلع نيست

Biometrics خصوصيات يكتاي فيزيكي – اثر انگشت

Time-stamping مهر زماني – شاهد(شخص ثالث)

Trusted Third party شخص ثالث مورد اعتماد

Digest خلاصه پيام - امضاء

Symmetric متقارن – استفاده از يك كليد متقارن براي رمز و رمزگشايي پيام

Asymmetric نامتقارن – استفاده از كليد عمومي و خصوصي براي رمز و رمز گشايي پيام ها

Security Attacks حملات امنيتي

Security Services سرويسهاي امنيتي

Security Mechanism ازسازوكارهاي امنيتي

Interruption قطع- قطع ارتباط پيام در بين راه و عدم وصول پيام

Fabrication

ايجاد پيغام – ارسال يك پيام جديد ازطرف سيستم ثالث غيرمجاز به كاربر، بدون اينكه پيامي وجود داشته باشد

Modification دستكاري دادهها – تغيير داده ها توسط سيستم ثالث غير مجاز در بين راه ارسال پيغام

Interception	دسترسي غيرمجاز- دسترسي سيستم ثالث غير مجاز به اطلاعات ارسالي
auditing	ممیزي
encryption	رمزنگاري
Privacy	حريم خصوصي- محرمانگي
Hash	توابع درهم سازي
Asymmetric	الگوريتمهاي نامتقارن
(Symmetric	الگوريتمهاي متقارن
PIN (Personal Identity Number)	شماره هويت فردي
Digital signature	امضاي ديجيتالي
Message	پيام
Certification Authority	مركزصدورگواهي
Root CA	مركز صدور گواهي ريشه
Intermediate CA	مركز صدور گواهي مياني
Secure Socket Layer-SSL	لايه امن سوكت
PKI – Public Key Infrastructure	زير ساخت كليد عمومي
CA – PKI	نظام تائيد هويت الكترونيكي
ISMS-Information Security Management System	سيستم مديريت امنيت اطلاعات
BS۷۷۹۹	استاندارد مديريت امنيتي انگليس
Security Policy	سياستهاي امنيتي
Accountability	پاسخگويي
Security Awareness	آگاهي رساني امنيتي
Authority	حدود اختيارات
Physical Protection	محافظت فيزيكي
Availaibility	قابليت دسترسي
Vulnerability	آسيب پذيري

Functionality Test	تست عملكرد
Intrusion نفوذ	
Concernنگراني	
Monitoring نظارت	
Inappropriate نامناسب	
Denial of Service ممانعت از سرويس	
Concept مفهوم	
Common Criteria معيارهاي مشترك	
Responsibility مسئوليت	
Risk management مديريت مخاطره	
Security officer مدير امنيت	
Malicious مخرب	
Containmentمحدود سازي	
Certification گواهي	
Access control كنترل دسترسي	
Steering Committeeكميته راهبري	
Password كلمه عبور	
Worm كرم	
Reliability قابليت اطمينان	
Content Filtering فيلترينگ محتوي	
Constraint فشار	
UnAuthorize غير مجاز	
Informal غير رسمي	
Classification طبقه بندي	
Weakness ضعف	

Third party شخص ثالث

Virtual Private Network (VPN) شبکه خصوصي مجازي

Intrusion Prevention system سيستم پيشگيري از نفوذ

Intrusion detection system سيستم تشخيص نفوذ

Information Security امنيت اطلاعات

Asset سرمايه

Complianceسازگاري

Infrastructure زير ساختار

Residual risk ريسك باقيمانده

Encryption رمز نگاري

Strategy راهبرد

Categorization دسته بندي

Loss خسارت

Disasterخرابي

Incidents حوادث

Safeguard حفاظ

Life Cycle چرخه حيات

Framework چار چوب

Threat تهديد

Recommendation توصيه

Security organization تشكيلات امنيت

Disaster Recovery ترميم خرابي

Security Training تربيت نيروي انساني در زمينه امنيت

Instant Messaging پيام رساني فوري

Prevention پيش گيري

Scanner پويشگر

Promiscuous بي قاعده

Compliance checking بررسي سازگاري

Recovery بازيابي

Audit بازرسي

Feedback باز خورد

Objectives اهداف قطعي

Goals اهداف نهايي

Disiplinary انظباطي

Risk Analysis آناليز مخاطره

Security Education آموزش امنيت

Preparation آماده سازي

Redundancy افزونگي

Assurance اطمينان

Evaluation ارزيابي

Assessment ارزيابي

Authority اختيار