Sikkerhetsmål er altså egenskaper ved informasjonssikkerhet, egenskaper vi ønsker å oppnå eller tilby, og som på sett og vis beskriver informasjonssikkerhet.

a) Konfidensialitet
Konfidensialitet betyr at informasjon ikke tilgjengeliggjøres for annet enn de entiteter, systemer og/eller prosesser som er autorisert for tilgang til informasjonen. Det kan gjelde forretningshemmeligheter, personopplysninger, eller å f.eks. sikre anonymitet der dette er nødvendig. Konfidensialitet omfatter alle typer informasjon/data, alt fra forretningshemmeligheter, personopplysninger til konfigurering av systemer og da data som er med på å styre datamaskiner.

Som sikkerhetstiltak benyttes kryptering (lagring og kommunikasjon), tilgangskontroll (god styring på hvem som har tilgang til hva) og det som kalles skallforsvar (hindre uvedkommende tilgang innenfor et "skall", jmfr et godt gjerde rundt en bygning. Helseopplysninger er eksempler på konfidensielle opplysninger som skal beskyttes særlig.

Tilgangskontroll er et viktig sikkerhetselement. Det avgjør hvem som har tilgang til hvilke data, apper og ressurser – og under hvilke omstendigheter. På samme måte som nøkler og forhåndsgodkjente gjestelister beskytter fysiske områder, beskytter policyer for tilgangskontroll digitale områder.

b) Integritet
Integritet handler om å kunne stole på at informasjon eller systemer ikke er endret eller slettet av entiteter, systemer eller prosesser som ikke er autorisert for handlingen. Brudd på integritet kan skyldes både angre7p utenfra og feil i systemer som fører til korrupte data. I likhet med konfidensialitet omfatter integritet også alle typer informasjon/data.

Som tiltak er autentisering og logging av andringer viktig, dessuten kryptering, gjerne i form av hash-algoritmer ved deling av data, samt digitalt signert programvare. Når du f.eks. skal laste ned programvare fra nett får du ofte programvaren sammen med en sjekksum, slik at du selv kan sjekke om programvaren stemmer med sjekksummen etter nedlastning (sikrer både mot korrupt programvare og nedlastingsfeil).

c) Tilgjengelighet
Tilgjengelighet dreier seg om at informasjon til enhver tid skal være tilgjengelig for den som skal ha tilgang til informasjonen. Mobilnett, nødnett, pasientsystemer, banksystemer, betalingssystemer er viktige systemer vi i dag er forholdsvis avhengige av i hverdagen, og som dermed bør ha sterkt fokus på tilgjengelighet. Samtidig vil det for en nettbutikk føre til svikt i omsetningen hvis deres nettbutikk gjøres utilgjengelig for en periode, selv om det kanskje ikke berører oss forbrukere på samme måte (vi velger en annen butikk...). DDOS-angrep eller andre angrep som tar ned et system/en tjeneste er en trussel, men det samme er f.eks. systemfeil, naturkatastrofer eller strømbrudd.

Som sikkerhetstiltak benyttes gjerne backup (av både informasjon og programvare, slik at gjenoppretting blir enkelt, samt å ha redundante systemer tilgjengelig.

d) Autentisering
Autentisering er å sikre at alle parter er de som de utgir seg for å være, f.eks. ved passord. F.eks. at nettsiden du besøker er den nettsiden du mente å besøke, og ikke en identisk kopi.

Hovedtrusselen er at noe eller noen klarer å utgi seg for å være noen/noe de ikke er. Passord er f.eks. enkelt å stjele/gjette/knekke, og falske nettsider ganske enkelt å lage. Som sikkerhetstiltak benyttes

først og fremst ulike autentiseringsfaktorerog kryptografiske protokoller. Dette kommer vi nærmere inn på i forelesning om autentisering.

e) Uavviselighet (tidligere ikke-fornektelse).

Det skal ikke være mulig å påstå at man ikke har gjort noe man har gjort, og at man har gjort noe man ikke har gjort. Dette gjelder f.eks om man har undertegnet en kontrakt (f.eks. for boliglån), eller glemmer å overføre penger i nettbanken.

Uavviselighet er altså å bekrefte at en handling eller et informasjonselement er uendret (integritet) og at det kan knyttes til en bestemt identitet. Uavviselighet er i mange sammenhenger også omtalt om ikke-benekting. En løsning for uavviselighet er en løsning som gjør det mulig for også en tredjepart å innhente tilstrekkelig dokumentasjon for at en annen part ikke kan nekte for å ha gjennomført en handlig eller ha valgt å bekrefte/vedgå seg et informasjonselement.

En løsning for uavviselighet er bygget opp på samme måte som løsninger for autentisering. Forskjellen er at brukeren skal være i stand til ikke bare å bekrefte hvem man er over nettet, men også å legge igjen dokumentasjon som entydig knytter personen til en handling eller et uendret informasjonselement.

f) Sporbarhet

Sporbarhet, også omtalt som etterprøvbarhet, er egenskapen som sikrer at alle handlinger kan spores tilbake til en entydig entitet. Sporbarhet garanterer at alle operasjoner som utføres av individer (brukere, personer, systemer eller prosesser som kjøres kan identifiseres, og at sporene bevares (logges) for senere bruk.

Ved et datainnbrudd øker dette muligheten for å spore en kriminell handling tilbake til den eller de som utfører handlingen. Men fortsatt er det dessverre slik at det på tvers av landegrenser, uten felles lovverk, kan være svært vanskelig å stille gjerningsmenn til ansvar for kriminelle handlinger.

Å sørge for sporbarhet i et system vil i mange tilfeller også være med på å rette opp feil som skjer. Et eksempel er, som nevnt på forelesning, hvis du plutselig oppdager at karakteren din plutselig er endret fra en ståkarakter til stryk, uten grunn. I et system som sikrer sporbarhet vil denne endringen kunne spores, og handlingen knyttes til f.eks. en identifiserbar bruker. Personen vil kunne stilles til ansvar for handlingen, og man kan finne ut om det er en feil, sabotasje, el.

For å kunne sikre sporbarhet brukes de preventive tiltakene autentisering og logging, mens etterforskning er et tiltak som benyttes i etterkant, som et korrigerende tiltak når en hendelse er avdekket og man må nøste i hva som har skjedd og til slutt "rydde opp".