Institutionen för Data- och Systemvetenskap
Stockholms Universitet

Ordinarie Tentamen 2015-10-28, 4,5 av 7,5 poäng

Kursbeteckning:	SÄK1
Kursnamn:	Informationssäkerhet - modeller och synsätt
Ansvarig:	Dr. Fredrik Björck
Tid:	2015-10-28, 0900-1300 (4 timmar)

Regler

- Tentamen kan ge totalt 100 poäng. Varje fråga ger 2 poäng.

- Inga hjälpmedel utöver översättningslexikon, penna, radergummi, samt kladdpapper (papper distribuerats av vakterna för den som behöver).

- Med översättningslexikon avses en bok som listar ord på svenska för översättning till ett annat språk, men dock utan att ordens betydelse ytterligare förklaras.

- Svaren avges på det separata svarsarket genom att ange ett tydligt kryss för det svarsalternativ som du väljer.

- Varje fråga har fyra svarsalternativ av vilket endast ett är rätt och ger poäng. Du måste välja endast ett.

- Det är inget poängavdrag för att chansa, så chansa alltid om du inte kan – det kommer att fungera i genomsnitt i cirka en ¼-del av fallen. En bra metod om du inte kan se svaret direkt är ”uteslutningsmetoden”: Ta först bort det eller de alternativ du vet är fel. Om fler alternativ återstår, chansa på det du tycker verkar troligast.

- Om det från examinators sida är oklart vilket svarsalternativ som markerats, så ges inga poäng för den frågan. Det är därför av största vikt att alltid radera ut tidigare svar vid ändring.

- Facit utgörs av a) Litteraturen (dock ej referenslitteraturen), b) Föreläsningsbilderma, och c) det som sagts på föreläsningarna. Om du anser att dessa källor är inkonsistenta på någon punkt, så gäller de i den ordningen de uppräknades.

- Frågorna *kan* innehålla tvetydigheter och flera av svarsalternativen *kan* vara mer eller mindre korrekta. I sådana fall skall du välja det svarsalternativ som är *mest* rätt, enligt det som lärts ut i kursen – det är endast detta alternativ som ger poäng.

Vi önskar dig lycka till på provet! Vänd på sidan för att börja provet *efter* klartecken.

Till tentamensvakt
Bläddra igenom eventuella medtagna översättningslexikon för att säkerställa att det inte finns anteckningar eller noteringar direkt i böckerna eller i lösblad, samt att de inte innefattar ytterligare förklaringar av ordens betydelse. Var idag extra vaksamma på att studenterna inte tittar på varandras svarsark eftersom tentamen är av flervalstyp. Varje student ska efter provet lämna tillbaks svarsark SAMT tentamensfrågorna för att kunna få tentamen rättad.

Fråga 1: Vilket av följande ingår normalt *inte* i en *verksamhetsanalys* i samband med informationssäkerhetsarbete:

a) Att analysera risker

b) Att identifiera informationstillgångar

c) Att fastställa krav på informationssäkerheten

d) Att diskutera lagkrav relaterade till informationssäkerhet

Fråga 2: Vilka analyser krävs innan man kan sägas ha en god bild av *skyddsbehovet* för information (med skyddsbehov avses i vilken utsträckning man har behov av att skydda informationen)?

a) Riskanalys och Gapanalys

b) Endast verksamhetsanalys

c) Endast Gapanalys

d) Verksamhetsanalys och riskanalys

Fråga 3: Vilken av följande aktiviteter är normalt *inte* en del av en riskanalys?:

a) Identifiera hot mot informationstillgångarna

b) Bedöm sannolikhet för att risken ska inträffa

c) Bedöm konsekvens ifall risken inträffar

d) Klassificera informationstillgången

Fråga 4: Vad är målet med informationssäkerheten i en affärsdrivande verksamhet?

a) En balans mellan säkerhet och skydd.

b) Högsta möjliga säkerhet (att sträva efter detta).

c) Att säkerheten skall bidra till verksamhetens överlevnad och vinst.

d) Att nå den punkt då kostnaden för säkerhet är exakt lika stor som värdet av informationstillgångarna som skall skyddas.

Fråga 5: Vad är det främsta resultatet av en *riskanalys*?

a) En beskrivning av verksamhetens informationssäkerhetsnivå.

b) En uppfattning om de mest relevanta riskernas (sannolikhet och konsekvens)

c) En lista på samtliga kritiska informationstillgångar.

d) En beskrivning av den planerade riskmiljön.

Fråga 6: Vilken av följande innefattar de *fyra informationssäkerhetsmål* som togs på föreläsningarna?

a) Tillgänglighet, konfidentialitet, riktighet, autenticitet

b) Riktighet, tillgänglighet, sekretess, dataskydd

c) Konfidentialitet, riktighet, spårbarhet, tillgänglighet

d) Ingen av ovanstående

Fråga 7: Vad innebär *tillgänglighet* inom informationssäkerhet?

a) Det innebär att information och IT-system inte *avslöjas* eller görs tillgängliga för obehöriga.

b) Det innebär att information eller system inte felaktigt *förändras* av misstag eller av obehörig.

c) Det innebär att informationen är *korrekt* (med sanningen överensstämmande).

d) Det innebär att informationen *kan nås* av den som är behörig och behöver den.

Fråga 8: *Spårbarhet* gällande händelser i ett IT-system får man främst genom:

a) Att genomföra så kallad systemspårning

b) Att bibehålla sekretessen

c) Att införa inloggning

d) Att logga händelser

Fråga 9: Vad menas med *administrativt* skydd?

a) Åtgärder för att främja informationssäkerheten och som är ekonomiskt rationella.

b) Åtgärder som bland annat ska påverka beteende.

c) Åtgärder som brandväggar, behörighetskontrollsystem och antivirusprogram.

d) Åtgärder som inte kräver någon närmare analys innan man inför dem.

Fråga 10: Med ”informationstillgångar” avses:

a) En organisations informationsrelaterade tillgångar, vilka utgör ett värde och därmed är skyddsvärda.

b) De tillgångar som behandlas med informationsteknik (IT).

c) De informationsresurser som en viss anställd har tillgång till.

d) En organisations tillgångar som ej är av fysisk karaktär.

Fråga 11: I ”Introduction to the systems approach” beskriver författarna något de kallar den ”subsystem”. Vad menar de med det?

a) En delmängd av den samling element som utgör systemet i vilken samtliga ursprungliga relationer mellan dessa element är *förändrade*.

b) En delmängd av den samling element som utgör systemet i vilken samtliga ursprungliga relationer mellan dessa element är *oförändrade*.

c) *Samtliga* element som utgör systemet *men* där de ursprungliga relationerna mellan dessa element är *förändrade*.

d) *Samtliga* element som utgör systemet *men* där de ursprungliga relationerna mellan dessa element är *oförändrade*.

Fråga 12: Ett perspektiv på system kallas för ”svart låda” (”black box”). Vad innebär det?

a) Att man tar ett internt och därmed förenklande perspektiv på systemet.

b) Att varje system behöver någon typ av delsystem som ansvarar för spårbarhet.

c) Att man ser systemet utifrån och därmed förenklande.

d) Att alla systemets miljöfaktorer ska samlas i en ”svart låda” för bättre överskådlighet.

Fråga 13: Vad kan systemteori användas för inom informationssäkerhet?

a) Analys av endast *tekniska* system

b) Analys av endast *sociala* system (bestående av människor)

c) Analys av *alla typer av system* som kan förekomma inom informationssäkerhet

d) Analys av endast *administrativa, logiska och fysiska* system

Fråga 14: Vad kallas den roll i Personuppgiftslagen som ett *företag* eller en *organisation själv* har vad gäller hantering av personuppgifter:

a) Personuppgiftsombud (PUL-ombud)

b) Personuppgiftsbiträde (PUL-biträde)

c) Personuppgiftsansvarig (PUL-ansvarig)

d) Personuppgiftschef (PUL-chef)

Fråga 15: Vad är en *personuppgift* i personuppgiftslagens mening?:

a) Endast de uppgifter som företag hanterar om sina kunder

b) Alla uppgifter som kan hänföras till en person

c) Uppgifter om personligheter

d) Det är omöjligt att säga generellt

Fråga 16: Vid behandling av *personuppgifter* i enlighet med personuppgiftslagen ska nivån på säkerheten för att skydda uppgifterna anpassas till … :

a) … de integritetsrisker behandlingen medför.

b) … hur känsliga de behandlade personuppgifterna är.

c) … vilka tekniska möjligheter som finns och vad det kostar att genomföra dem.

d) Samtliga ovanstående alternativ (a, b och c).

Fråga 17: Vilket begrepp betyder: ”Attribut utan vilka ett objekt eller en relation skulle beskrivas så som det är?:

a) Definierande attribut

b) Att man kan klara sig utan relationen

c) Beroende relation

d) Beroende attribut

Fråga 18: Vilket av följande var ett av de huvudsakliga målen med Generell Systemteori (GST)?

a) Att främja vetenskapen genom tillväxt av kunskap.

b) Att överföra resultat från en disciplin (kunskapsområde) till ett annat.

c) Att framföra att människor egentligen uppvisar stora likheter med djuren (och andra sociala varelser).

d) Att främja kunskapen inom analytiska och systemiska angreppssätt.

Fråga 19: Vilket av följande är *inte* del av en definition av ett systems *miljö* inom systemteorin?:

a) Något som påverkar systemet

b) Något som ligger utanför systemet

c) Något som ligger innanför systemet

d) Något utanför systemets direkta kontroll

Fråga 20: Churchman beskriver fem grundläggande karaktärsdrag vilka system har. Ett av dem är att de är *målsökande*. Ett annat ord för målsökande är:

a) Teleopatisk

b) Telepatisk

c) Teleforisk

d) Teleologisk

Fråga 21: Antag att två system sägs vara *analoga* i jämförelse med varandra, och två andra system sägs vara *isomorfa*. Vad är skillnaden?

a) Analoga system har *samma* miljö, medan ismorfa har *olika* miljöer.

b) **Analoga system *liknar* varandra, medan isomorfa *även* består av motsvarande element.**

c) Analoga system har *olika* miljöer, medan ismorfa har *samma* miljö.

d) Det är ingen skillnad – begreppen betyder i stort sett samma sak.

Fråga 22: Bouldings fem postulat inom generell systemteori tar alla upp … :

a) Kaos

b) Ordning

c) Miljön

d) Tillit

Fråga 23: Vilken av följande utsagor har med *ekvifinalitet* att göra?:

a) Alla tentor är ungefär lika svåra att studera till, om man ser till helheten.

b) Det finns flera olika sätt att studera, vilka leder till samma goda resultat.

c) I slutändan spelar det stor roll hur mycket man studerat.

d) Ingen av de ovanstående (a, b eller c).

Fråga 24: Ett öppet system …

a) Har i regel färre hierarkier än ett slutet system.

b) Är ändå oftast stängt med avseende på informationsresurserna.

c) Importerar resurser från miljön, och exporterar slutprodukten till miljön.

d) Har ingen egentlig miljö eftersom allt (principiellt sett hela universum) ingår i miljön.

Fråga 25: Vad är sant rörande ett stängt system (closed system)?

a) Ingen transformationsprocess kan ske inom systemet eftersom det är helt isolerat.

b) Inget kan föras in eller ut ur systemet.

c) Om ett fel sker blir det alltid mer omfattande, och får större konsekvenser än i ett öppet system.

d) Stängda system har (per definition) inga informationstillgångar att skydda.

Fråga 26: Stafford Beer, om han levat, skulle betecknat en organisation bestående av människor som

a) Ett probabilistiskt (baserat på sannolikhet) och ytterligt komplext system.

b) Ett levande och deterministiskt system för samarbete.

c) Ett probabilistiskt men ändock relativt enkelt system.

d) Ett deterministiskt men komplext system.

Fråga 27: Enligt Beer, vilken typ av kontroll krävs för att kontrollera ett *komplext deterministiskt* system?

a) Något som kontrollerar *transformationerna*.

b) Något som kontrollerar *utflödet* (resultatet).

c) *Ingen* kontroll krävs.

d) Något som kontrollerar *inflödet.*

Fråga 28: Med återkoppling (feedback) avses inom cybernetiken att…

a) Signalen kopplas tillbaks för att ytterligare öka effekten.

b) Effekten kopplas tillbaks för att ytterligare höja signalen.

c) Signalen återförs från ett senare (output) till ett tidigare stadium (input).

d) Signalen förs från ett tidigare (input) till ett senare stadium (output).

Fråga 29: Inom cybernetikens kontrollsystem, vad avses med *positiv återkoppling*?

a) Det är då differensen mellan verkligt och önskat värde initierar åtgärd för att få kontroll, för att återgå till önskat värde.

b) Det är återkoppling som är fördelaktig för kontrollsystemet.

c) Det är då en del av utflödet förs tillbaks och sedan adderas till inflödet – skapar tillväxt av den kontrollerade variabeln snarare än håller den konstant.

d) Det är återkoppling som inte är till fördel för kontrollsystemet.

Fråga 30: Vilken typ av kontrollsystem kan reflektera över tidigare fattade beslut, är självorganiserande och lärande?

a) *Första* ordningens kontrollsystem (first order)

b) *Andra* ordningens kontrollsystem (second order)

c) *Tredje* ordningens kontrollsystem (third order)

d) *Både* b och c har sådana egenskaper

Fråga 31: Kontrollsystemet måste kunna uppvisa minst lika många olika lägen som det kontrollerade systemet har, om man skall kunna vara säker på att man verkligen har kontroll, enligt …?

a) *Ashbys lag* om tillräcklig variation (requisite variety)

b) *Beers lag* om tillräcklig variation (requisite variety)

c) *Bouldings lag* om tillräcklig variation (requisite variety)

d) Den så kallade *kontrollprincipen* inom generell systemteori

Fråga 32: Beers *tredje kontrollprincip* säger att *icke-kontroll initierar åtgärder för att* …?

a) Minska kontrollen

b) Förbättra kontrollsystemet

c) Återfå kontrollen

d) Fastställa systemets mål

Fråga 33: Vad är skillnaden mellan manuella och automatiska kontrollsystem?

a) Manuella kräver mänsklig intervention, till skillnad från automatiska.

b) Automatiska kontrollerar fler variabler än manuella.

c) Automatiska är i regel mer effektiva än de manuella.

d) Manuella är i regel mer effektiva än de automatiska.

Fråga 34: Institutionell teori kan endast tillämpas när det man vill analysera uppvisar någon form av:

a) säkerhetsbrist

b) socialt beteende

c) juridisk avvikelse

d) avvikande beteende

Fråga 35: Föreläsaren Björck argumenterade på kursen att *graden av säkerhet i alla informationssystem bestäms i slutändan av …*?

a) administratörens kunskap

b) människors handlande

c) den tekniska utvecklingen

d) användaren

Fråga 36: Institutioner definierades i kursen som *strukturer baserade på mer eller mindre för givet tagna regler* vilka begränsar och kontrollerar (eller stöder) socialt beteende. Vilka typer av regler avses?

a) Formella regler

b) Informella regler

c) Formella *och* informella regler

d) Ingen av ovanstående

Fråga 37: Scott beskriver i sin three pillars-modell (tre pelare) tre olika typer av institutioner, nämligen …?

a) Regulativa, Normativa och Kognitiva

b) Regulativa, Normativa och Legala

c) Regulativa, Normativa och Kulturella-kognitiva

d) Informella, Formella och Tekniska

Fråga 38: Vilket av följande alternativ beskriver en institution vilken är av *normativ* typ?

a) Styrs av moral

b) Styrs av lag

c) Styrs av kultur (värderingar)

d) Styrs av *både* lag och kultur

Fråga 39: Till vad kan man använda institutionell teori inom informationssäkerhet?

a) Förstå och förklara skillnaden mellan formella regler och faktiskt beteende

b) Förstå och förklara varför vissa aktörer har avancerade regler som inte efterlevs

c) Förstå, förklara och försöka styra/påverka beteende så att det blir ”säkrare”

d) Institutionell teori kan användas för samtliga ovanstående ändamål

Fråga 40: Vad är menas med ett teckens *konnotation* inom Semiotiken?

a) Det tecknet direkt refererar till

b) Tecknets kontext (dess sammanhang)

c) **Det tecknet indirekt refererar till**

d) Tecknets form

Fråga 41: Vilken av följande är *inte* en del av den semiotiska ”stegen”?

a) Syntax (Syntactics)

b) Semantik (Semantics)

c) Elektronik (Electronics)

d) Pragmatik (Pragmatics)

Fråga 42: Om vad handlar *semantik* inom semiotiken?

a) Handling

b) Mening

c) Strategier

d) Bandbredd

Fråga 43: Den semiotiska stegen kan sägas ha olika fokus på olika nivåer. Antag att du ska analysera en elektronisk kommunikation mellan två personer. Vilket av följande är korrekt?

a) På *lägre* nivåer i stegen är är det mer *handling* än på högre nivåer

b) På *högre* nivåer i stegen är det mer teknikfokus än på lägre nivåer

c) Lägre nivåer handlar mer om den elektroniska kommunikationen medans den övre handlar om människorna som kommunicerar

d) Man kan inte analysera en elektronisk kommunikation med den semiotiska stegen eftersom den enbart handlar om kommunikation mellan människor

Fråga 44: Vilken nivå på den semiotiska stegen handlar bland anat om formella strukturer, grammatik och logik?

a) Sociala världen

b) Semiotik

c) Semantik

d) Syntax

Fråga 45: Standarden ISO/IEC 27001:2013 används *främst* för att …?

a) Hantera *alla* typer av incidenter

b) Styra informationssäkerhet i organisationer

c) Styra informationssäkerheten för en individs behov

d) Leda ett företags *generella* kvalitetsarbete

Fråga 46: Vilken av följande var *inte* en av de *externa aktörerna* inom informationssäkerhet, som togs upp på kursen?

a) Hotande aktörer (t.ex. hackers)

b) Opinionsbildande aktörer (t.ex integritetsivrande föreningar)

c) Beslutande aktörer (t.ex. ett företags verkställande direktör)

d) Övervakande aktörer (t.ex. finansiell revisor)

Fråga 47: En lag om informationssäkerhet är ett exempel på ….?

a) Ett externt krav

b) Ett internt krav

c) Ett extrovert krav

d) Ett introvert krav

Fråga 48: Vad menas med *semantisk analys* i samband med exempelvis systemutveckling?

a) Det finns inget som heter så

b) En analys som egentligen inte hade behövts utföras

c) Utredning av behovet av kommunikation

d) Begreppsutredning

Fråga 49: Ett system definieras som:

a) En uppsättning objekt inklusive relationer mellan dessa och mellan dessas attribut.

b) En uppsättning objekt inklusive relationer mellan dessa och mellan dessas attribut, relaterade till varandra och till deras miljö för bildandet av en huvuddel.

c) En uppsättning objekt inklusive relationer mellan dessa och mellan dessas attribut, relaterade till varandra och till deras miljö för bildandet av en helhet.

d) En uppsättning objekt inklusive relationer mellan dessa och mellan dessas avvikelser, relaterade till varandra och till deras miljö för bildandet av en huvuddel.

Fråga 50: På kursen togs olika *typer* av skydd eller säkerhetsåtgärder upp, som en organisation kan använda för sin informationssäkerhet. Vilka var det?

a) Logiska, pragmatiska och empiriska säkerhetsåtgärder

b) Logiska, pragmatiska och administrativa säkerhetsåtgärder

c) Sociala respektive tekniska säkerhetsåtgärder

d) Logiska, fysiska samt administrativa