Certifieringsregler för

Information Security Management Professional (ISMP)

RISE Research Institutes of Sweden AB
Certifiering - Certification
2017-10-02

Förord

Certifiering innebär bestyrkande från en oberoende tredjepart att personen uppfyller krav i standard eller annan form av specifikation. Certifiering av personer vid RISE baseras på standarden SS-EN ISO/IEC 17024.

Denna certifieringsregel anger villkor för certifiering av Information Security Management Professional (ISMP).

Certifieringsregeln är framtagen med hjälp av en referensgrupp. Referensgruppen består av relevanta intressenter i den aktuella branschen. Revidering av certifieringsregeln kan bli aktuell som en följd av erfarenheter av certifieringsregelns tillämpning. RISE äger certifieringsregeln.

I Sverige råder stor frihet på arbetsmarknaden för många yrkesgrupper att verka utan krav på yrkesbevis eller krav på fackutbildning. Genom att vi på RISE blir anlitade för att utföra oberoende granskningar och att ställa ut certifikat, kan vi på så sätt hjälpa till att validera och kvalitetssäkra yrkeskompetenser. Detta ger en ökad trovärdighet för yrkesutövarna, samtidigt som det kan skapa visshet för de certifierades uppdragsgivare.

Borås 2017-10-02

Dag Sjöholm

RISE Research Institutes of Sweden AB
Certifiering

Huvudkontor:
Box 857
SE-501 15 BORÅS
Sweden

Telefon +46 10 516 50 00
Fax +46 33 13 55 02
E-mail info@ri.se
Internet www.sp.se

Personcertifiering nås via
Box 553
SE-371 23 KARLSKRONA
Sweden

Telefon +46 10 516 63 00
Fax +46 455 206 88
E-mail fragor.person@ri.se
Internet www.sp.se/personcertifiering

Innehållsförteckning

1. Omfattning

Denna regler omfattar certifiering av personer i rollen som Information Security Management Professional (ISMP). Syftet med certifieringen är att visa att personen uppfyller kraven i denna certifieringsregel.

1.1 Arbetsbeskrivning

Arbetsuppgiften för en certifierad ISMP är primärt att analysera och utforma, införa och förvalta ledningssystem för informationssäkerhet liksom säkerhetsåtgärder samt att utföra revision inom området. Tillämpliga kunskapsområden gäller styrning, säkerhetsåtgärder, riskhantering och revision med utgångspunkt i standarderna ISO 27000, 27001, 27002, 27005, 27007, 27008 och SS-EN ISO 19011 samt EU-direktiv och förordningar relaterade till informationssäkerhet.

1.2 Bakgrund

Denna certifieringsordning togs ursprungligen fram av det nationella standardiseringsorganet SIS och dess tekniska kommitté TK 318 på uppdrag av SIS Förlag AB med stöd av MSB, FMV, Stockholms universitet, NSD samt föreningarna SIG Security och SAISec. Under 2015 avyttrade SIS certifieringsordningen till RISE Certifiering, vilka numera är huvudman för certifieringen.

Användningen av olika tekniker för informationsbehandling liksom mängden information som behandlas ökar hela tiden. Samhället blir alltmer beroende av att system för informations-behandling fungerar och att känslig information skyddas. Informationssäkerhetsområdet blir därför allt viktigare liksom behovet av personer som behärskar området. Flera aktörer, bland annat den Europeiska Nätverks- och Informations-säkerhetsmyndigheten ENISA har uttalat vikten av att etablera en personcertifiering som bygger på europeiska förhållanden. Inom informationssäkerhetsområdet finns inom EU ett antal direktiv och förordningar som medlemsländerna ska införa i form av nationell lagstiftning. Samtliga EU:s direktiv och förordningar finns publicerade på websidan www.eur-lex.europa.eu. Dessa berör till exempel följande områden:

- skydd av personuppgifter
- regler kring dataintrång
- datalagring för tele- och internetoperatörer
- rapportering av så kallade integritetsincidenter
- upphovsrätt och närstående rättigheter till information
- säkerhetskrav kring elektronisk kommunikation
- elektronisk autentisering och identifiering
- hantering av operativa risker inom olika branscher

Informationssäkerhetsarbetet i medlemsländerna sker inom denna legala kontext. Europa har ett starkt fokus på de internationellt vedertagna standarderna i ISO/IEC 27000-serien. Detta gör att en europeisk certifiering behövs och efterfrågas.

Andra aktörer, exempelvis europeiska och nationella standardiseringsorgan, och personcertifieringsaktörer i Europa, kan ansluta sig till certifieringen genom att etablera motsvarande certifieringsprocess under ackreditering i respektive medlemsland.

2 Krav på utbildning, erfarenhet och kompetens

2.1 Utbildning

Akademisk kandidatexamen eller högre utbildning från högskola/universitet kan ge rätt till reduktion (substitut) av krav på 5 års arbetsliverfarenhet (se 2.2). All utbildning ska styrkas med betygskopior.

Meriterande högre utbildning är kandidatexamen eller högre från högskola eller universitet. De flesta utbildningsinriktningar accepteras som ger generell kompetens att analysera, sammanställa information, att dra relevanta slutsatser och att kommunicera. Bachelor-examen från utlandet accepteras också.

2.2 Arbetslivserfarenhet

Den sökande ska med intyg eller med annan verifierbar information styrka praktisk erfarenhet enligt ett av följande två alternativ:

1. 5 års relevant arbetslivserfarenhet (minst halvtid) krävs. Erfarenheten får vara maximalt 10 år gammal, räknat från ansökningsdatumet. Med relevant erfarenhet avses arbete inom minst 2 av områdena styrning, säkerhetsåtgärder, riskhantering och revision (se nedan), eller
2. 3 års relevant arbetslivserfarenhet (minst halvtid) för sökande med högre utbildning krävs. Erfarenheten får vara maximalt 10 år gammal, räknat från ansökningsdatumet. Med relevant erfarenhet avses arbete inom minst 2 av områdena styrning, säkerhetsåtgärder, riskhantering och revision (se nedan).

Med de fyra områdena avses följande:

a) Styrning enligt ISO 27000 och ISO 27001 samt tillämpliga EU-direktiv
b) Säkerhetsåtgärder enligt ISO 27005 samt tillämpliga EU-direktiv
c) Riskhantering enligt ISO 27005 samt tillämpliga EU-direktiv
d) Revision (som revisor) enligt ISO 19011, ISO 27007, ISO 27008 samt tillämpliga EU-direktiv

Erfarenheten styrks med tjänstgöringsintyg eller annan likvärdig dokumentation. Med intyg menas ett dokument som redovisar den sökandes erfarenhet, men har en annan person än den sökande som intygsgivare. Intygsgivaren kan vara arbetsgivare, uppdragsgivare eller annan betrodd person som har kompetens och möjlighet att utöva insyn i den sökandes yrkesbana. Certifieringsorganet kontrollerar regelbundet med stickprov att intygade uppgifter är med verkligheten överensstämmande.

2.3 Lämplighet

Lämplighet för uppgiften att vara Information Security Management Professional ska styrkas av den sökande med en signerad blankett ”Accepterande av Professionellt förhållningssätt”.

2.3.1 Krav på personliga egenskaper

SS-EN ISO 19011:2011 tillsammans med ISO/IEC 27007:2011 fastslår krav på personliga egenskaper för den som ska arbeta med revision av ledningssystem för informationssäkerhet. Dessa krav gäller för samtliga som söker certifiering. Främst gäller kraven sådant som kan hänföras till det etiska området. Med utgångspunkt i kraven har principer för ett professionellt förhållningssätt formulerats vilka en sökande ska acceptera, tillämpa och förespråka.

2.3.2 Professionellt förhållningssätt

För att erhålla certifiering ska den sökande förbinda sig att acceptera, tillämpa och förespråka följande principer:

- **Uppträdande:** Att i sitt värv uppträda på ett oklanderligt och värdigt sätt.
- **Objektivitet:** Att tillämpa ett objektivt synsätt där problem och potentiella lösningar bedöms utifrån olika perspektiv.
- **Lojalitet:** Att utföra uppdrag lojalt, ändamålsenligt och i enlighet med uppdragsgivarens instruktioner utan att åsidosätta samhällets bästa.
- **Konfidentialitet:** Att inte obehörigen röja information man fått del av genom uppdrag eller anställning.
- **Kultur:** Att vara lyhörd för, och ta hänsyn till, kulturella skillnader mellan olika typer av verksamheter och geografiska platser.
- **Integritet:** Att i förekommande fall påtala brister, felaktigheter, och etiska tveksamheter i uppdrag eller arbetsuppgifter på ett tydligt och konstruktivt sätt.
- **Lagstiftning:** Att hålla sig informerad om och tillämpa gällande lagstiftning inom informationssäkerhetsområdet.
- **Standarder:** Att förespråka användning av standarder och vedertagen praxis inom området.

3 Certifieringsprocessen

3.1 Allmänt

För att bli certifierad som ISMP behöver aktiviteterna i nedanstående certifieringsprocess följas. Vissa aktiviteter åligger den sökande att utföra och andra aktiviteter åligger RISE att utföra.

3.2 Ansökan

Ansökan sker i följande steg:

a) Den sökande ansöker om certifiering via ansökan som finns på RISE webbplats under personcertifiering. I och med att ansökan skickas in accepteras ”RISE allmänna villkor” och ”Generella villkor för personcertifiering” samt RISE hantering av personuppgifter (PUL).
b) Den sökande faktureras en ansökningsavgift.
c) Den sökande får tillgång till RISE kundportal genom en aktiveringskod som skickas ut efter ansökan. Den sökande loggar in till RISE kundportal och laddar där upp intyg och andra dokument som krävs för bedömning av den sökandes kompetens för certifiering.

3.3 Granskning av ansökan

Vid granskningen av ansökan kontrollerar RISE att ansökan är komplett, och att ansökan kan hanteras inom reglerna. Den sökandes redovisade kompetens bedöms av RISE certifieringsingenjör. Om certifieringsingenjören bedömer att ansökan inte är fullständig behöver den sökande komplettera med ytterligare information eller dokument. Utöver granskning av ansökan krävs att den sökande har skrivit ett godkänt kunskapsprov i regi av RISE (se examination) för att bli certifierad.

3.4 Examination - tentamen

Examination innebär att kandidaten genomgår kunskapsprövning. Prövningen sker i form av tentamen. För att kunna bli certifierad ska denna prövning vara slutförd med godkänt resultat. Denna prövning bokas via RISE eller via utbildningsföretag som RISE har avtal med.

3.4.1 Krav på godkänt resultat

Kandidaten ska styrka sin kunskap inom området genom att uppnå godkänt resultat på en grundläggande tentamen som består av flervalsfrågor och essäfrågor. Tentamen tillhandahålls av RISE. För att uppnå godkänt resultat ska kandidaten klara 70 % av maxpoängen. Kraven på godkänt resultat gäller vid nyansökan och förnyelseansökan (vid omcertifiering).

Om kandidaten inte uppfyller kraven på godkänt resultat vid tentamen för nyansökan och förnyelseansökan kan omtentamen ske. Omtentamen ska äga rum inom 6 månader från första tentamenstillfället. Efter 3 underkända tentamen måste kandidaten ha ett uppehåll på minst 1 år innan ny omtentamen kan ske. Ny tentamen upprättas vid varje omtentamen.

Vid förnyelse av certifiering har den sökande rätt till förenklad kunskapsprövning under förutsättning att den sökande har arbetat halvtid inom meriterande områden enligt kapitel 2.2 under tidigare certifieringsperiod.

3.5 Granskning och beslut

När granskningen av kandidatens kompetens är färdigbehandlad lämnas ärendet över till en certifieringsingenjör som inte har varit involverad i certifieringen för beslut. När ett beslut är fattat skickar RISE ut beslutsbeskedet och papperskopia på certifikatet om kandidaten valt detta i sin ansökan. Aktuell status i handläggningen av ärendet går alltid att utläsa i kundportalen.

När beslut om certifiering är fattat kan den certifierade kunden logga in på kundportalen för att ladda hem ytterligare kopia på certifikatet. Får kandidaten avslag på ansökan om certifikat redovisas skälen för detta. Kandidaten har möjlighet att överklaga beslutet i enlighet med ”Generella villkor för personcertifiering”.

3.6 Certifikatets giltighet och årsrapportering

Giltighetstiden för certifikatet är fem år. Certifikatet gäller under förutsättning att certifikatsinnehavaren årligen har sänt in årsrapport till RISE som redovisar arbetslivserfarenhet som ISMP samt dokument/intyg på eventuellt genomförd fortbildning.

Även ”nollrapportering” ska lämnas in, det vill säga om certifikatsinnehavaren inte haft några uppdrag eller utbildningar under certifieringsperioden. Det är certifikatsinnehavarens ansvar att bevaka de datum som gäller för certifikatets giltighet och att höra av sig till RISE i god tid för förnyelse av certifikatet. I regel är dock RISE behjälpliga med detta.

3.7 Förnyelse av certifiering

När innevarande certifieringsperiod går ut för ett certifikat har certifikatsinnehavaren möjlighet att certifiera om sig för en ny period. Förnyelse kan göras inom ett år efter att tidigare certifiering gått ut. Förnyelsen följer samma process som vid en ny ansökan om certifiering, vilket innebär att den sökande genomgår kapitel 3.2 – 3.5.

Vid ansökan om förnyelse ska den sökande skicka in:

a) Ansökan om förnyelse, se kapitel 3.2
b) Årsrapport för det senaste året, se kapitel 3.6
c) Lämplighetsintyg, se kapitel 2.3
d) Intyg om genomförd godkänd tentamen, se kapitel 3.4

För denna granskning fakturerar RISE en ansökningsavgift.

För att få rätt till förnyelse ska den certifierade under den tidigare certifieringsperioden ha arbetat minst halvtid med minst två av de fyra områdena som beskrivs i kapitel 2.2. Eventuell utbildningstid räknas in i arbetstid.

Specialfall: Vid sjukdom, föräldraledighet och andra liknande skäl, kan RISE i enskilt fall efter bedömning besluta att kravet är uppfyllt trots att arbetstiden understiger det föreskrivna.

3.8 Förändringar i certifieringen

Innehavaren av certifikatet ska utan dröjsmål informera RISE om ändringar i förhållanden som kan påverka förmågan att uppfylla kraven för certifieringen.

När det sker ändringar i certifieringsregeln som kräver ytterligare utvärdering kommer RISE att informera om vad som krävs av den certifierade för att uppfylla de ändrade kraven.

4 Övriga villkor för certifiering

Det är möjligt att rapportera klagomål mot en person som RISE har certifierat. Klagomålet ska vara skriftligt och ska handla om brister som har en tydlig koppling till kraven i denna certifieringsregel. RISE bekräftar till den klagande om klagomålet är relaterat till aktiviteter som RISE är ansvarig för. Om klagomålet är betydande informerar RISE även den certifierade personen. RISE utreder klagomålet och den klagande får information under utredningens gång. Beslut i klagomålet fattas av en person som inte har varit involverad i det uppdraget som klagomålet avser. Beslutet meddelas den klagande. Civilrättsliga tvister hanteras av domstol. Klagomål mot RISE certifieringsbeslut eller avslag om certifiering hanteras av RISE Certifieringsstyrelse.

Utfärdat certifikat kan återkallas av RISE, tillfälligt eller definitivt, om villkoren för certifieringen inte är uppfyllda. Detta och andra specifika villkor för personcertifiering framgår av ”Generella villkor för personcertifiering” i RISE INFO 2012:03.

En person med giltigt certifikat har möjlighet att marknadsföra detta genom att använda certifieringsmärket eller logotyp från RISE. Villkor för användningen av märken och logotyper framgår av information på RISE webbplats alternativt kan informationen erhållas direkt från RISE. När certifikat upphör att gälla, upphör personens eller företagets rätt att marknadsföra certifikatet.

5 Referenser

SS-EN ISO/IEC 17024 Bedömning av överensstämmelse – Krav på organ som certifierar personer