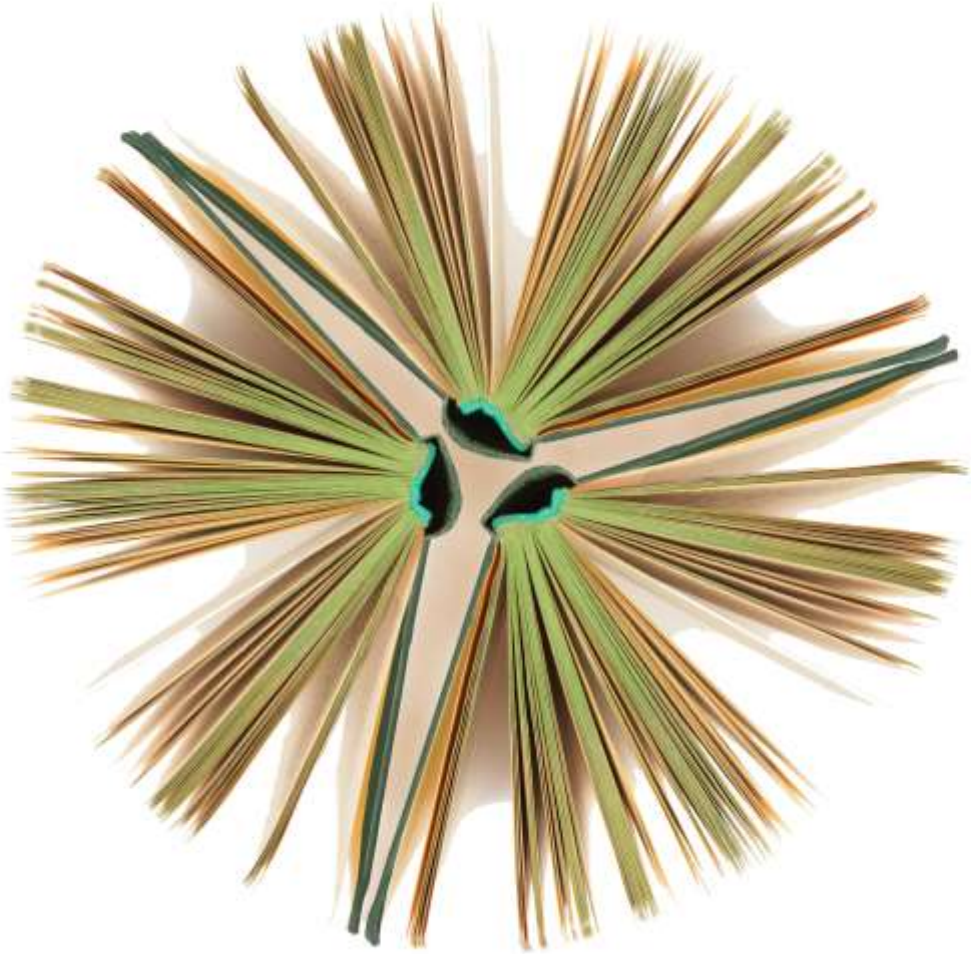
Deloitte.



Þróun ISO 27001 og núverandi staða

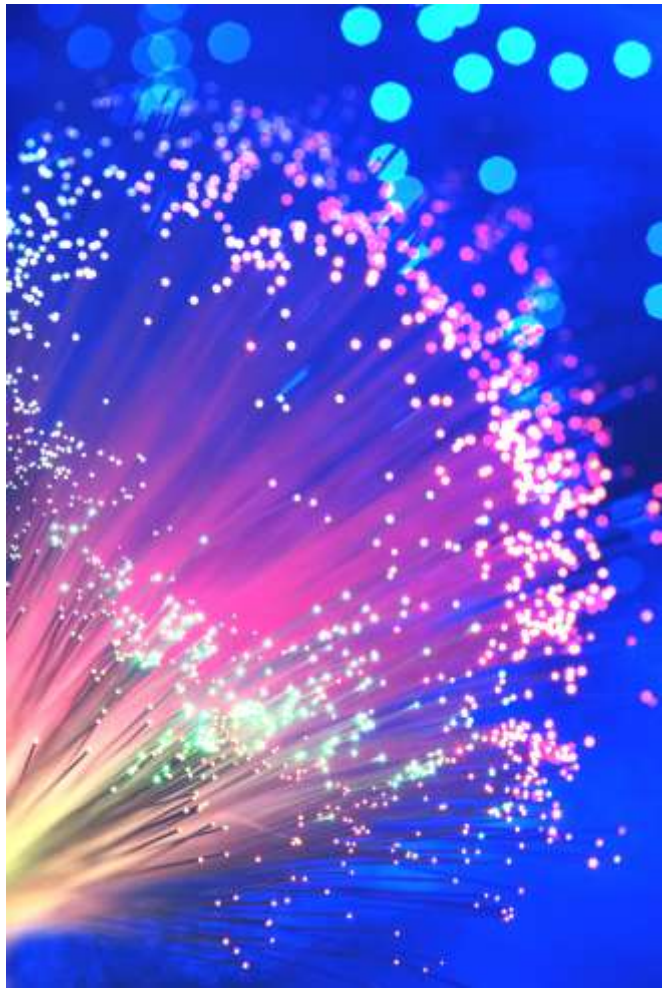
Einar Ragnar Sigurðsson
Öryggisstjóri Deloitte ehf

3. október 2018

Þróun ISO 27001 og nú verandi staða

... með áherslu á fyrirbyggjandi aðgerðir

1. Hvaða staðlar eru þetta og hvaðan koma þeir?
2. Hvernig hafa staðlarnir þróast?
3. Hvað er í þessum stöðlum?
4. Hvernig beitum við stöðlunum við fyrirbyggjandi aðgerðir?
5. Er vottunin sjálf fyrirbyggjandi?



Hvaða staðlar eru þetta?
ISO 27001 og ISO 27002

ISO 27001

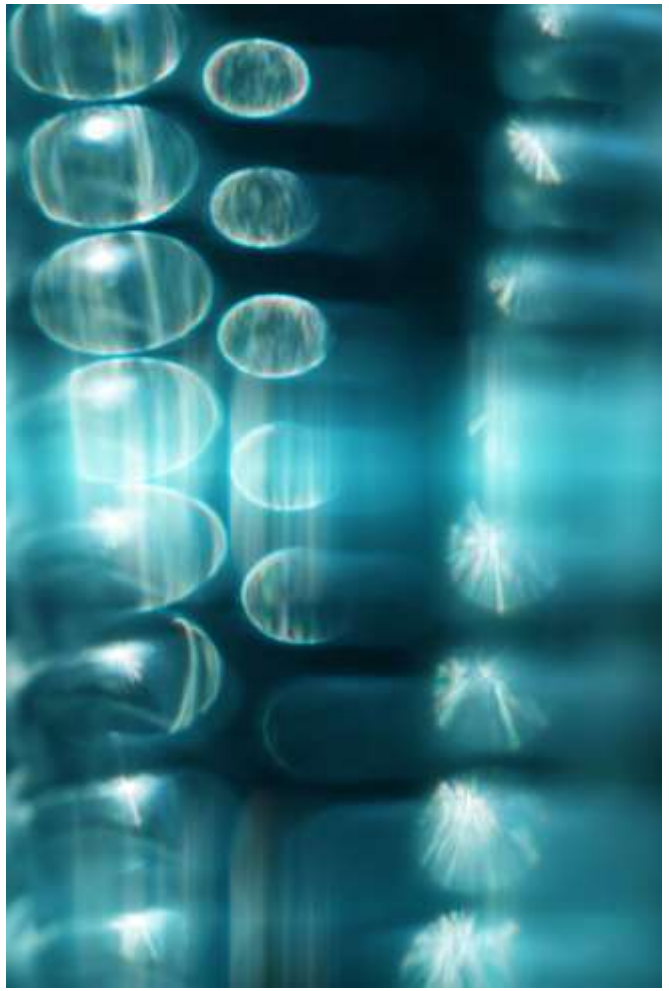
- Kröfur til stjórnunarkerfis upplýsingaöryggis
- Kröfustaðallinn sem vottað er eftir
- Segir hvað skuli vera til staðar og hvað skuli gera ef vottun á að nást.

ISO 27002

- Leiðbeiningar um hvað ætti að gera og hvernig ætti að standa að innleiðingu stýringa í staðlinum – Controlin

ISO 27000

- Skilgreiningar og umgjörð utan um hvaða staðlar þetta eru



Hvaðan koma þeir?

Í upphafi var BS7799 og jafnvel eitthvað annað á undan því!

ISO 27002: Leiðbeiningar um innleiðingu stýringa (controlin)

- Gefinn út af BSI árið 1995 sem BS 7799 part 1: best practices for Information Security Management
- Upprunninn áratugum fyrr í tölvudeildum stórfyrirtækja (Shell). „Code of Practice for Information Security Management”
- Varð árið 2000 að ISO 17799
- Endurskoðun ISO 17799:2005
- Númerabreyting með ISO 27002:2005
- Núverandi útgáfa ISO 27002:2013
- ÍST EN ISO/IEC 27002:2017

- BS = British Standard

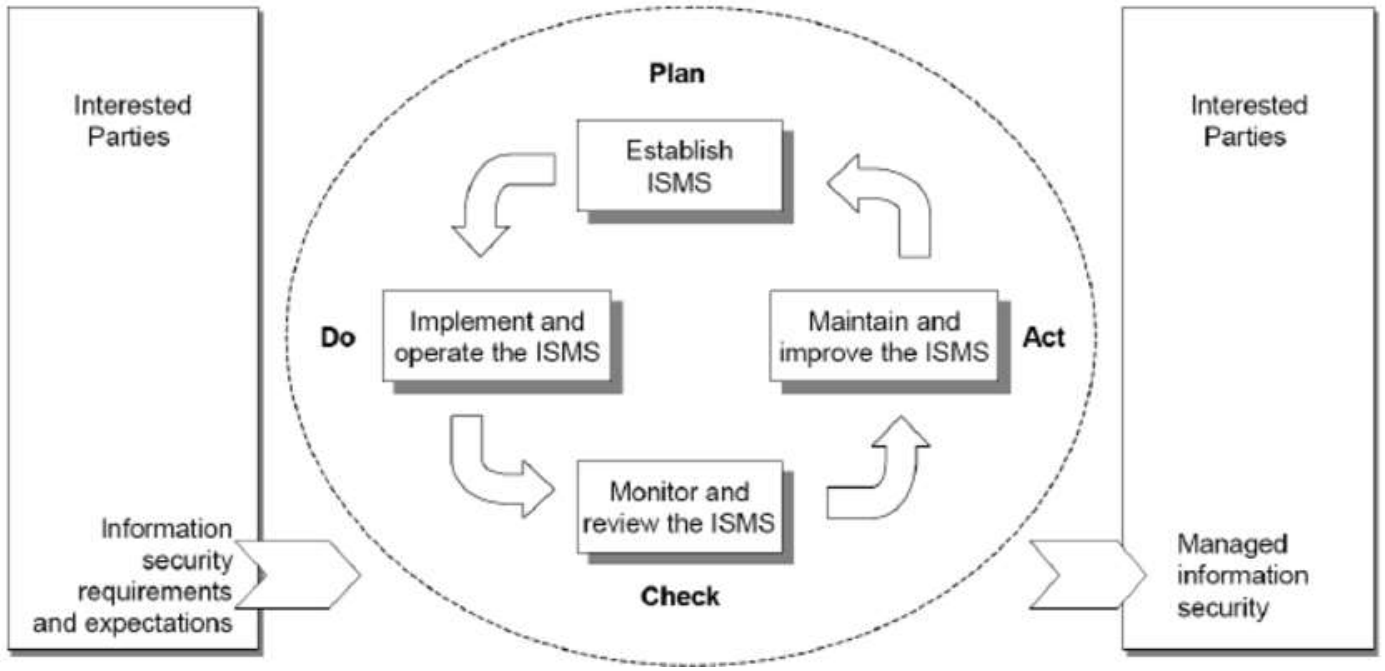
ISO 27001: Kröfur til stjórnunarkerfis og þá staðallinn sem er vottað eftir

- BS 7799 part 2, Information Security Management Systems - Specification with guidance for use. Útgáfa 1999
- Endurskoðaður árið 2002 með PDCA aðferðafræðinni
- Varð árið 2005 að ISO 27001
- ÍST EN ISO/IEC 27001:2017

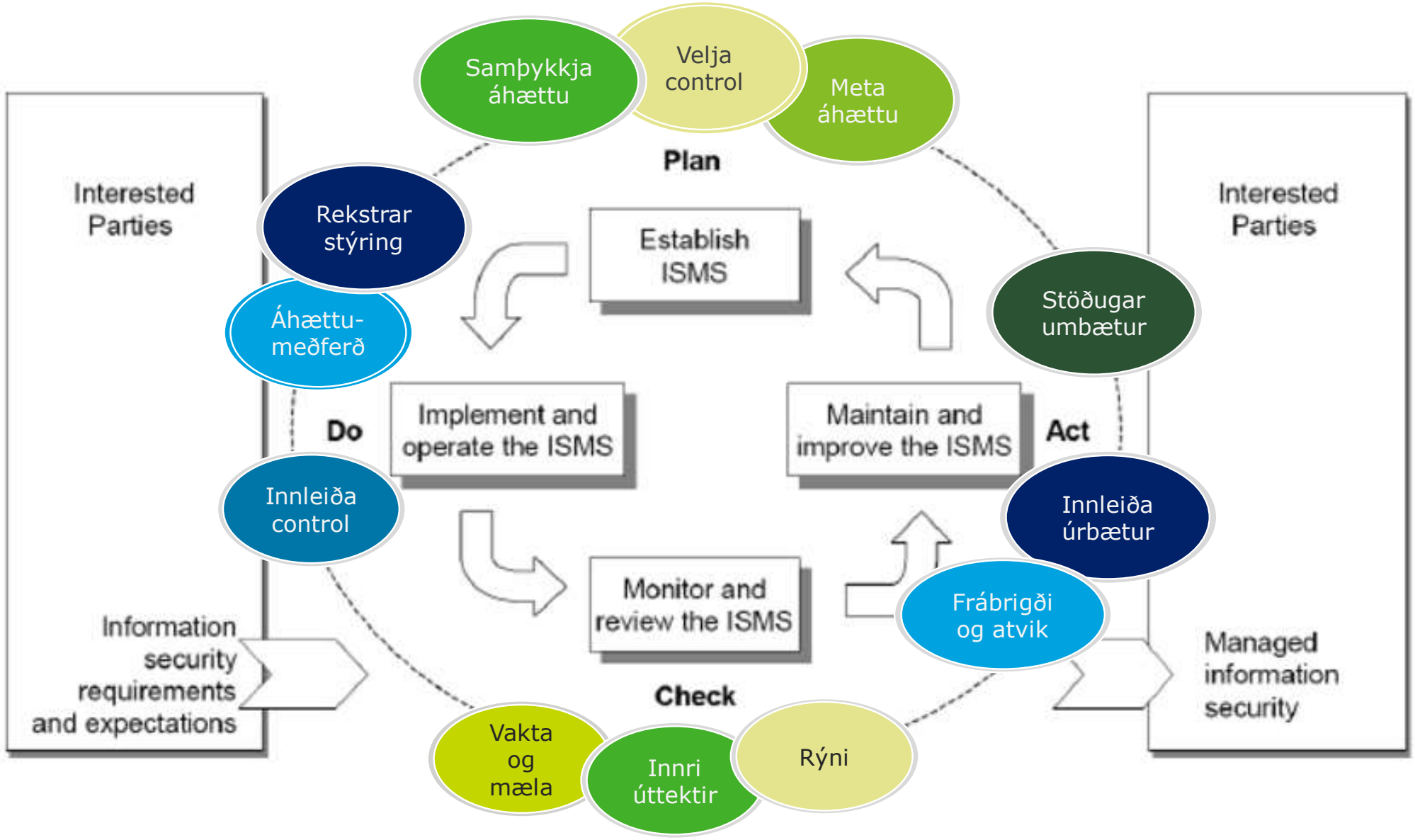
Tengsl við ISO 9000 staðla um gæðastjórnun og PDCA aðferðafræðin

Hvort kom á undan eggið eða hænan?

- ISO 9000 staðlarnir líka upprunnir hjá BSI sem BS 7750 frá 1979
  - BS7750 og ISO 9001 með gæðastýringu fyrir framleiðslufyrirtæki
  - BS7799 tæknilegar leiðbeiningar til að tryggja öryggi í upplýsingatækni
- Þróuðust báðir í anda Plan-Do-Check-Act hugmyndafræði gæðastjórnunar



PDCA líkanið og áhersla á fyrirbyggjandi aðgerðir



Annex SL

Samræming stjórnunarstaðla til vottunar

1. Scope
2. Normative references
3. Terms and definitions
4. Context of the organisation
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance evaluation
10. Improvement

Plan

Do

Check

Act

1. Umfang
2. Tilvísanir í staðla
3. Hugtök og skilgreiningar
4. Samhengi skipulagsheilar / fyrirtækis
5. Forysta
6. Skipulagning
7. Stuðningur
8. Rekstur
9. Mat á frammistöðu
10. Umbætur

Hvernig lítum við á ISO 27000 staðlana ?

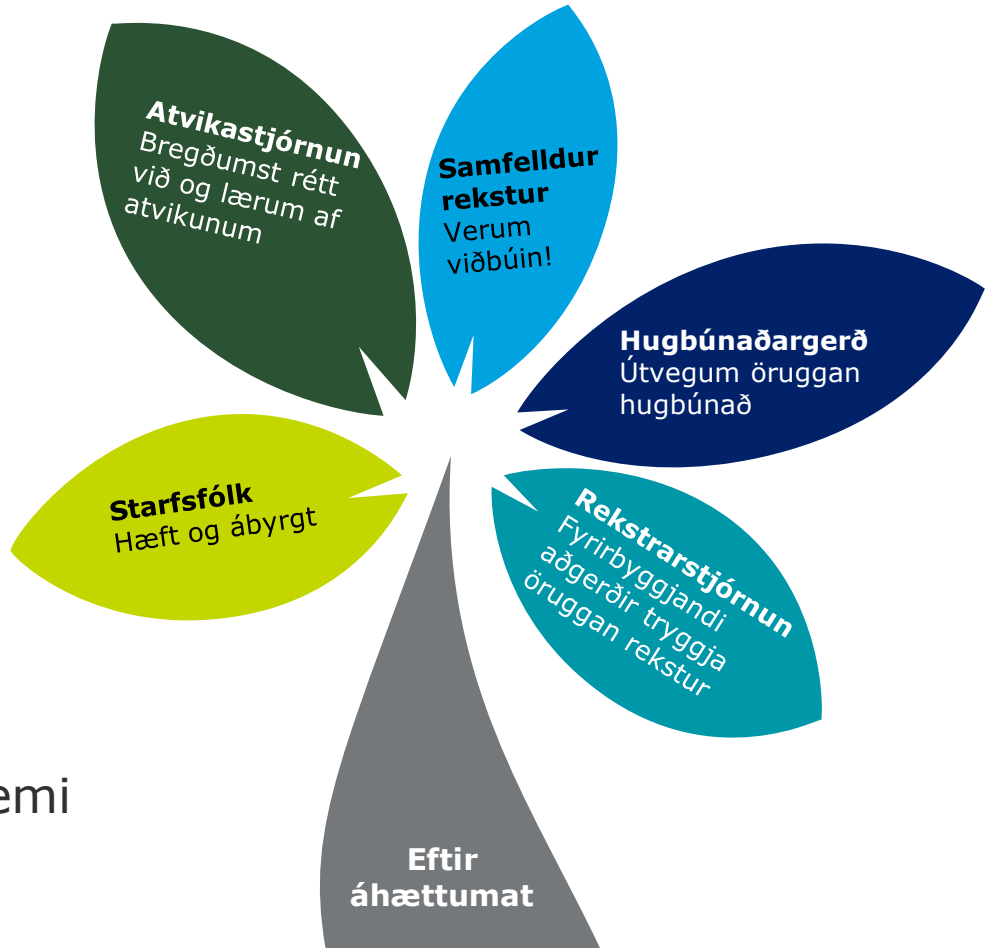
Þetta er e.t.v. bara spurning um nálgun

- Fullt af skjölum sem þarf að gera
- Fullt af controlum sem þarf að innleiða
- Áhættumatið getur verið lykillinn að góðu kerfi

- Samræmt stjórnunarkerfi miðað við Annex SL
  - ISO 27001
  - ISO 9001
  - ISO 14001
  - og um 20 aðrir staðlar !

Fyrirbyggjandi control ISO 27002

Staðallinn er fyrirbyggjandi í heild sinni. Verum búin að byrgja brunninn.



Nokkur dæmi

Starfsfólk (A7)
Þjálfun og val starfsfólks til að minnka líkur á því sem við viljum ekki að gerist.

Rekstrarstjórnun (A 12 og 13)
Rétt upp sett kerfi, rétt pötsuð og rétt afrituð. Ákveðum fyrirfram hvaða logga þarf að færa og pössum þá

Að útvega hugbúnað (A14)
Gerum kröfur, vitum hvaða öryggi þarf í kerfunum okkar. tryggjum að kröfurnar séu uppfylltar. Hvort sem við búum kerfin til eða aðrir gera það fyrir okkur.

Atvikastjórnun (A16)
Lærum af atvikunum sem verða þannig að við grípum til fyrirbyggjandi aðgerða og minnkum líkur á að þau endurtaki sig.

Samfelldur rekstur (A17)
Vinnum heimavinnuna og vitum nákvæmlega hvernig við ætlum að bregðast við ef alvarleg áföll dynja yfir.

Að fá vottun skv. ISO 27001

Er það fyrirbyggjandi aðgerð?

Það sem vottunin felur í sér

- Þarf að uppfylla allar kröfur stjórnkerfis ISO 27001
- Innleiða þau control sem eiga við
  - SOA: Statement of appliccability
    Yfirlýsing um nothæfi
- Ytri þrýstingur út af vottuninni
- Vissan um að það sé búið að gera það sem þarf að vera búið að gera
- Fyrirbyggjandi ?

Deloitte.