Archwilio Cymru
Audit Wales

Cylch gorchwyl: Y Pwyllgor Archwilio a Sicrwydd Risg

Blwyddyn archwilio: 2020-21

Dyddiad cyhoeddi: Ebrill 2020

Fersiwn: TERFYNOL

Mabwysiadwyd gan y Pwyllgor: 9 Mehefin 2020

Cymeradwywyd gan y Bwrdd: 11 Mehefin 2020

Archwilio Cymru yw enw ymbarél Archwilydd Cyffredinol Cymru a Swyddfa Archwilio Cymru, sy'n ddau endid cyfreithiol ar wahân â'u swyddogaethau cyfreithiol eu hunain. Mae gan yr Archwilydd Cyffredinol swyddogaethau archwilio ac adrodd ar gyrff cyhoeddus yng Nghymru. Mae gan Swyddfa Archwilio Cymru swyddogaethau i ddarparu adnoddau, megis staff, i arfer swyddogaethau'r Archwilydd Cyffredinol, ac i fonitro a chynghori'r Archwilydd Cyffredinol. Nid yw Archwilio Cymru yn endid cyfreithiol ac nid oes ganddo unrhyw swyddogaethau.

Un o bwyllgorau Swyddfa Archwilio Cymru yw'r Pwyllgor Sicrhau Risg ac Archwilio.

Cynnwys

Cylch gorchwyl

Y Pwyllgor Archwilio a Sicrwydd Risg

Statws

1 O dan adran 29 o Ddeddf Archwilio Cyhoeddus (Cymru) 2013, caiff rheolau trefniadol Swyddfa Archwilio Cymru ddarparu ar gyfer sefydlu pwyllgorau y gall Bwrdd Swyddfa Archwilio Cymru ddirprwyo unrhyw rai o'i swyddogaethau iddynt.

2 Yn ei gyfarfod cyntaf ar 23 Hydref 2013, sefydlodd Bwrdd Swyddfa Archwilio Cymru Bwyllgor Archwilio a Rheoli Risg i gynorthwyo'r Bwrdd a'r Swyddog Cyfrifyddu drwy adolygu hyd a lled a dibynadwyedd y sicrwydd a geir o ran llywodraethu, rheoli risg, yr amgylchedd rheoli, ac uniondeb y datganiadau ariannol a'r adroddiad blynyddol. Yn ei gyfarfod ar 23 Mai 2014, penderfynodd y Bwrdd newid ei enw i'r Pwyllgor Archwilio a Sicrwydd Risg.

Nod

3 Nod y Pwyllgor yw rhoi cyngor i'r Bwrdd o ran a yw trefniadau archwilio a sicrwydd risg Swyddfa Archwilio Cymru:

a) yn cefnogi ei nodau strategol;

b) yn sicrhau bod modd cyflawni busnes yn effeithlon, yn effeithiol ac yn ddarbodus;

c) yn cydymffurfio â'r gofynion rheoleiddiol.

4 Mae'r Pwyllgor yn bodloni'r nod hwn drwy:

a) adolygu hyd a lled a dibynadwyedd y sicrwydd a geir er mwyn bodloni anghenion y Bwrdd a'r Swyddog Cyfrifyddu;

b) adolygu uniondeb y datganiadau ariannol a'r adroddiad blynyddol, gan gynnwys y datganiad llywodraethu blynyddol;

c) rhoi barn ar y graddau y mae'r Bwrdd a'r Swyddog Cyfrifyddu'n cael eu cynorthwyo i benderfynu ac i gyflawni eu rhwymedigaethau stiwardiaeth ac atebolrwydd.

Cyfrifoldebau

5 Mae'r Pwyllgor yn rhoi cyngor i'r Bwrdd a'r Swyddog Cyfrifyddu ar hyd a lled a dibynadwyedd trefniadau sicrwydd Swyddfa Archwilio Cymru, gan gynnwys:

a) y trefniadau asesu risg a rheoli risg, yn enwedig adolygu'r pethau a ganlyn a rhoi cyngor arnynt –

(i) y strategaeth risg, gan gynnwys pa mor briodol yw'r dull a ddefnyddir gan Swyddfa Archwilio Cymru i bennu faint o risg y mae'n barod i'w hysgwyddo

(ii) prosesau asesu risg cyffredinol Swyddfa Archwilio Cymru sy'n gosod sail ar gyfer penderfyniadau gweithredol

(iii) gallu Swyddfa Archwilio Cymru i bennu ac i reoli risg

(iv) cylch gwaith y swyddogaeth rheoli risg, gan gynnwys ei gallu i gael mynediad at adnoddau a gwybodaeth i gyflawni ei rôl yn effeithiol ac yn unol â'r safonau proffesiynol perthnasol, heb i'r rheolwyr nac unrhyw beth arall ei rhwystro

(v) pa mor barod yw'r rheolwyr i ymateb i asesiadau risg;

b) rheoli risgiau seiber, gan gynnwys strategaethau priodol i liniaru'r risgiau (atodiad 2);

c) uniondeb y datganiadau ariannol, gan gynnwys –

(i) cysondeb y polisïau cyfrifyddu ac unrhyw newidiadau iddynt

(ii) y dulliau a ddefnyddir i gyfrif am drafodiadau sylweddol neu anarferol lle mae ffyrdd eraill o weithredu'n bosibl

(iii) a yw Swyddfa Archwilio Cymru wedi dilyn safonau cyfrifyddu priodol a gwneud amcanestyniadau a dyfarniadau priodol, gan ystyried barn yr archwilydd allanol

(iv) eglurder yr wybodaeth a ddatgelir yn yr adroddiad blynyddol a'r cyfrifon a'r cyd-destun y gwneir y datgeliadau hynny ynddo

(v) yr holl wybodaeth o sylwedd a ddarperir gyda'r datganiadau ariannol

(vi) yr arsylwadau a wnaed a'r sicrwydd a gafwyd yn eu cylch yn sgil gweithgarwch a chanlyniadau archwiliadau mewnol ac allanol;

d) yr amgylchedd rheoli mewnol, gan gynnwys effeithiolrwydd rheolaethau ariannol a systemau rheoli risg mewnol Swyddfa Archwilio Cymru, a'r datganiadau i'w cynnwys yn yr adroddiad blynyddol a'r cyfrifon

e) y trefniadau llywodraethu, yn enwedig –

(i) pa mor ddigonol a diogel yw trefniadau Swyddfa Archwilio Cymru i sicrhau bod modd i'w chyflogeion a'i chontractwyr fynegi pryderon, yn gyfrinachol, am gamymddwyn posibl o ran adroddiadau ariannol neu faterion eraill, gan gynnwys a ydynt yn caniatáu i faterion o'r fath fod yn destun ymchwiliad cymesur ac annibynnol a chamau dilynol priodol

(ii) gweithdrefnau Swyddfa Archwilio Cymru i atal ac i ganfod twyll

(iii) systemau a rheolaethau Swyddfa Archwilio Cymru i atal llwgrwobrwyo ac i gael adroddiadau am ddiffyg cydymffurfiaeth

(iv) adroddiadau rheolaidd gan y Swyddog Adrodd Gwyngalchu Arian a pha mor ddigonol ac effeithiol yw systemau a rheolaethau Swyddfa Archwilio Cymru i atal gwyngalchu arian.

f) y trefniadau archwilio mewnol, yn enwedig –

(i) effeithiolrwydd swyddogaeth archwilio mewnol Swyddfa Archwilio Cymru yng nghyd-destun y system rheoli risg gyffredinol

(ii) penodi a diswyddo pennaeth y swyddogaeth archwilio mewnol

(iii) cylch gwaith y swyddogaeth archwilio mewnol, gan gynnwys ei gallu i gael mynediad at adnoddau a gwybodaeth i gyflawni ei rôl yn effeithiol ac yn unol â'r safonau proffesiynol perthnasol, heb i'r rheolwyr nac unrhyw beth arall ei rhwystro

(iv) y cynllun archwilio mewnol blynyddol

(v) adroddiadau i'r Pwyllgor gan yr archwilydd mewnol

(vi) parodrwydd y rheolwyr i ymateb i ganfyddiadau ac argymhellion yr archwilydd mewnol;

g) y trefniadau archwilio allanol, yn enwedig –

(i) y broses o benodi archwilwyr allanol er mwyn i'r Bwrdd gyflwyno argymhelliad i'w penodi i Bwyllgor Cyllid Senedd Cymru

(ii) y berthynas â'r archwilydd allanol

(iii) rhoi sylwadau ar y telerau cyflogi a chwmpas yr archwiliad

(iv) y cynllun archwilio blynyddol, gan sicrhau ei fod yn gydnaws â chwmpas yr archwiliad

(v) adolygu canfyddiadau'r archwiliad, gan gynnwys unrhyw broblemau mawr sydd wedi codi, unrhyw ddyfarniadau cyfrifyddu ac archwilio, maint y gwallau a bennwyd yn ystod yr archwiliad, ac effeithiolrwydd yr archwiliad

(vi) adolygu llythyrau sylwadau'r rheolwyr i'r archwilydd allanol

(vii) adolygu llythyr y rheolwyr ac ymateb y rheolwyr i ganfyddiadau ac argymhellion yr archwilydd

(viii) adolygu'r polisi o ran cyflenwi gwasanaethau nad ydynt yn rhai archwilio gan yr archwilydd allanol, gan ystyried unrhyw ganllawiau moesegol perthnasol.

6. Mae'r Pwyllgor yn rhoi cyngor i'r Bwrdd a'r Swyddog Cyfrifyddu pan fyddant yn gofyn amdano neu pan fydd yn teimlo ei bod yn briodol iddo wneud hynny.

Hawliau

7. Mae'r Bwrdd yn caniatáu i'r Pwyllgor:

a) ymchwilio i unrhyw weithgaredd sy'n rhan o'i gylch gorchwyl a rhoi sylwadau a chyngor ar drefniadau llywodraethu Swyddfa Archwilio Cymru;

b) cael gafael ar unrhyw ddogfennau neu wybodaeth arall gan staff Swyddfa Archwilio Cymru y mae eu hangen arno i gyflawni ei ddyletswyddau;

c) gyda chytundeb y Bwrdd, cael gafael ar y cyngor arbenigol allanol y mae ei angen arno, yn ei dyb ef, i gyflawni ei ddyletswyddau, gan gynnwys cael gafael ar wybodaeth ddibynadwy a chyfredol am drefniadau archwilio a rheoli risg sefydliadau eraill.

Aelodaeth

8 Aelodau'r Pwyllgor yw:

Alison Gerrard	-	Aelod anweithredol o'r Bwrdd
Anne Beegan	-	Aelod o'r Bwrdd a etholwyd o blith y cyflogeion
Dianne Thomas	-	Aelod allanol annibynnol
Isobel Everett	-	Cadeirydd anweithredol y Bwrdd

9 Mae'r Bwrdd wedi penodi Alison Gerrard yn Gadeirydd y Pwyllgor.

10 Y Bwrdd sy'n penodi aelodau i'r Pwyllgor, a hynny am gyfnod o hyd at bedair blynedd y gellir ei estyn am gyfnod arall o hyd at bedair blynedd. Pan fydd yn penodi'r Cadeirydd a'r aelodau, bydd y Bwrdd yn sicrhau bod gan y Pwyllgor yn ei gyfanrwydd yr holl sgiliau y mae eu hangen arno i gyflawni ei holl swyddogaethau.

Ysgrifenyddiaeth

11 Mae Ysgrifennydd y Bwrdd yn gweithredu fel ysgrifennydd i'r Pwyllgor ac mae'n gyfrifol am:

a) sicrhau bod y Pwyllgor wedi'i gyfansoddi'n briodol, ei fod yn cael cyngor priodol, a bod ei waith ef, y Bwrdd a phwyllgorau eraill y Bwrdd yn cael ei gydgysylltu'n glir;
b) trafod y rhaglen waith â'r Cadeirydd;
c) sicrhau bod y Pwyllgor yn cael gwybodaeth a phapurau'n brydlon er mwyn iddo ystyried y materion dan sylw yn llwyr ac yn briodol;
d) paratoi cofnodion drafft i'w cymeradwyo gan y Cadeirydd cyn eu dosbarthu i'r aelodau;
e) cadw cofnodion priodol o fusnes y Pwyllgor;
f) drafftio deunydd ar gyfer adroddiad blynyddol y Pwyllgor;
g) darparu unrhyw gymorth ymarferol arall sydd ei angen.

Cyfarfodydd

12 Mae'r Pwyllgor yn cwrdd o leiaf bedair gwaith y flwyddyn. Gall Cadeirydd y Pwyllgor gynnull cyfarfodydd ychwanegol yn ôl y gofyn. Gall aelodau'r Pwyllgor, Cadeirydd y Bwrdd, y Swyddog Cyfrifyddu, y Pennaeth Archwilio Mewnol neu'r archwilwyr allanol ofyn i'r Cadeirydd gynnull cyfarfodydd ychwanegol os ydynt yn tybio bod eu hangen. Ni chaiff y Cadeirydd wrthod unrhyw gais rhesymol.

13 Caiff cyfarfodydd y Pwyllgor eu galw gan yr ysgrifennydd ar gais y Cadeirydd. Oni chytunir fel arall, bydd yr ysgrifennydd yn anfon hysbysiad o bob cyfarfod at yr aelodau i gadarnhau'r lleoliad, y dyddiad a'r amser, ynghyd ag agenda o'r eitemau i'w trafod, a hynny o leiaf bum diwrnod gwaith cyn dyddiad y cyfarfod. Anfonir unrhyw bapurau ategol ar yr un pryd.

14 I gael cworwm i drafod busnes, bydd angen dau aelod (y Cadeirydd ac un arall). Bydd cyfarfod Pwyllgor a gafodd ei gynnull yn briodol a lle ceir cworwm yn gymwys

i arfer unrhyw awdurdod, pŵer a disgresiwn a freiniwyd yn y Pwyllgor neu y gall eu harfer, neu bob un ohonynt. Os na fydd Cadeirydd y Pwyllgor yn bresennol (ac ar yr amod bod yr holl aelodau eraill yn bresennol), gall yr aelodau sy'n weddill ethol un o'u plith i gadeirio'r cyfarfod.

15 Gall unrhyw aelodau nad ydynt yn gallu bod yn bresennol godi unrhyw bwyntiau gyda'r Cadeirydd cyn y cyfarfod y maent yn berthnasol iddo.

16 Bydd yr Archwilydd Cyffredinol yn rhinwedd ei rôl fel Swyddog Cyfrifyddu, Cyfarwyddwr y Gwasanaethau Corfforaethol, y Cyfarwyddwr Cyllid, y Pennaeth Archwilio Mewnol a chynrychiolydd yr archwilydd allanol yn mynd i gyfarfodydd y Pwyllgor. Gall y Pwyllgor ofyn i unrhyw rai o swyddogion eraill Swyddfa Archwilio Cymru fynd i'w gyfarfodydd i'w gynorthwyo â'i drafodaethau am unrhyw fater penodol.

17 Gall y Pwyllgor ofyn i unrhyw un neu bob un o'r rheini sydd fel rheol yn bresennol ond nad ydynt yn aelodau o'r Pwyllgor adael unrhyw ran o gyfarfod, neu gyfarfod cyfan, i hwyluso trafodaeth agored a di-flewyn-ar-dafod am faterion penodol; bydd y trafodaethau hynny'n cael eu cofnodi.

18 Bydd pob un o gyfarfodydd y Pwyllgor yn darparu ar gyfer trafodaethau preifat â'r Pennaeth Archwilio Mewnol a chynrychiolydd yr archwilydd allanol.

19 Gall y Bwrdd a'r Swyddog Cyfrifyddu ofyn i aelodau'r Pwyllgor roi mwy o gyngor tu allan i'r cylch cyfarfodydd ar faterion penodol o bryd i'w gilydd.

20 Bydd Cadeirydd y Pwyllgor yn cyfathrebu â Chadeirydd y Pwyllgor Tâl ac Adnoddau Dynol i gydgysylltu eu gweithgareddau a'u camau gweithredu fel y bo'n briodol.

21 Os bydd aelod o'r Pwyllgor neu rywun sy'n bresennol yn ei gyfarfodydd yn sylwi bod ganddo/ganddi fuddiant sy'n gwrthdaro, neu fuddiant a allai wrthdaro, o ran y materion a drafodir gan y Pwyllgor, dylai roi gwybod i'r Cadeirydd ymlaen llaw neu, os nad yw hyn yn bosibl, dylai ddatgan hynny yn y cyfarfod a, lle bo angen, dylai adael yr ystafell tra mae'r eitem berthnasol yn cael ei thrafod.

22 Yn eithriadol, gall y Pwyllgor dderbyn eitemau busnes tu allan i'r cylch cyfarfodydd arferol, er enghraifft os bydd mater annisgwyl yn codi y mae angen ymateb ar unwaith neu ar fyrder iddo. Bydd y trefniadau a nodir yn y cylch gorchwyl hwn o ran sicrhau cworwm, dosbarthu papurau a chofnodi trafodaethau'r Pwyllgor yn berthnasol.

Mynediad

23 Gall Cadeirydd y Pwyllgor ofyn i gael trafodaeth breifat â Chadeirydd y Bwrdd, y Swyddog Cyfrifyddu, y Pennaeth Archwilio Mewnol, staff Swyddfa Archwilio Cymru a chynrychiolydd yr archwilydd allanol fel y bo'n briodol.

24 Gall Cadeirydd y Pwyllgor hefyd gysylltu'n uniongyrchol â Chadeirydd Pwyllgor Cyllid Senedd Cymru a rhoi gwybod iddo/iddi am faterion sy'n peri pryder. Cyn arfer yr hawl hon, gall y Cadeirydd gyd-drafod, fel y bo'n briodol, â Chadeiryddion y

Bwrdd a'r Pwyllgor Tâl ac Adnoddau Dynol i drafod y pryderon a'r camau i'w cymryd.

25 Bydd y Pennaeth Archwilio Mewnol a chynrychiolydd yr archwilydd allanol yn gallu cael mynediad dirwystr a chyfrinachol at Gadeirydd y Pwyllgor Archwilio a Sicrwydd Risg.

Adrodd

26 Bydd y Pwyllgor yn rhoi adroddiad ysgrifenedig ffurfiol i'r Bwrdd a'r Swyddog Cyfrifyddu ar ôl pob cyfarfod.

27 Bydd y Pwyllgor yn rhoi adroddiad blynyddol ysgrifenedig ffurfiol i'r Bwrdd a'r Swyddog Cyfrifyddu sy'n crynhoi casgliadau'r gwaith y mae wedi ymgymryd ag ef yn ystod y flwyddyn. Bydd amseriad yr adroddiad yn cynorthwyo'r broses o gwblhau'r adroddiad blynyddol a'r cyfrifon.

Rhaglen fusnes

28 Mae Atodiad 1 yn crynhoi rhaglen fusnes y Pwyllgor a gaiff ei chadarnhau ym mhob cyfarfod.

Adolygu perfformiad, hyfforddiant a datblygu

29 Bydd y Cadeirydd yn adolygu perfformiad yr aelodau bob blwyddyn yn unol â'r fframwaith rheoli perfformiad a sefydlwyd at y diben hwnnw. Bydd Cadeirydd y Bwrdd yn adolygu perfformiad y Cadeirydd bob blwyddyn.

30 Bydd y Pwyllgor yn ystyried yn barhaus a oes angen darparu hyfforddiant cynefino neu gyfleoedd hyfforddiant a datblygu.

31 Bydd y Pwyllgor yn rhoi cyngor i'r Bwrdd am unrhyw ddiffygion ymddangosiadol y gall eu pennu o dro i dro o ran sgiliau cyfun ei aelodau.

Adolygu'r cylch gorchwyl

32 Bydd y Pwyllgor yn adolygu'r cylch gorchwyl hwn ac yn asesu ei effeithiolrwydd bob blwyddyn, gan roi gwybod am y canlyniad yn ei adroddiad blynyddol i'r Bwrdd.

Atodiad 1

Rhaglen fusnes

1. Mae rhaglen fusnes y Pwyllgor yn tybio y cynhelir cylch o bedwar cyfarfod y flwyddyn. Canllaw yw'r rhaglen a nodir isod ac nid yw'n atal y Pwyllgor rhag newid amseriad y trafodaethau yn ystod y flwyddyn nac ystyried unrhyw fusnes arall a allai godi.
2. Yr eitemau sefydlog ar agenda pob un o gyfarfodydd y Pwyllgor yw:
   a) cymeradwyo cofnodion cyfarfod blaenorol y Pwyllgor;
   b) log o gamau gweithredu sy'n codi o gyfarfodydd blaenorol y Pwyllgor wedi'i ddiweddaru fel y bo'n briodol (i'w drafod fel materion sy'n codi);
   c) rhaglen waith y Pwyllgor i'w hadolygu'n barhaus;
   d) adroddiad gan y Pennaeth Archwilio Mewnol sy'n crynhoi –
      - y gwaith a gyflawnwyd (a chymhariaeth â'r gwaith a gynlluniwyd)
      - unrhyw newidiadau i'r strategaeth archwilio mewnol a'r cynllun blynyddol
      - y prif faterion sy'n codi o'r gwaith archwilio mewnol
      - unrhyw broblemau o ran adnoddau sy'n effeithio ar y camau i gyflawni amcanion archwilio mewnol;
   e) adroddiadau archwilio mewnol yn unol â'r amserlen a bennwyd yn y cynllun archwilio mewnol ar gyfer y flwyddyn (gan gynnwys unrhyw ychwanegiadau a wnaed yn ystod y flwyddyn). Bydd yr adroddiadau'n cynnwys ymatebion y rheolwyr i'r argymhellion;
   f) adroddiad cynnydd (lle bo'n briodol) gan gynrychiolydd yr archwilydd allanol sy'n crynhoi'r gwaith a wnaed a'r canfyddiadau sy'n dod i'r amlwg;
   g) adolygiad risg strategol a ddefnyddir gan y Pwyllgor i bwyso a mesur un risg strategol mewn manylder i bennu a yw'r trefniadau rheoli risg yn gweithredu'n effeithiol o safbwynt ymarferol;
   h) adolygiad o'r map sicrwydd a ddefnyddir gan y Pwyllgor i bwyso a mesur un rhan o'r map mewn manylder.
   i) asesiad o berfformiad yr archwilwyr mewnol ac allanol.
3. Mae'r cylch busnes bras yn cynnwys:

   Cyfarfod 1 (Chwefror)

   - cylch gorchwyl y Pwyllgor i'w adolygu;
   - yr amserlen i baratoi'r adroddiad blynyddol a'r cyfrifon drafft;
   - y cynllun archwilio allanol ar gyfer yr adroddiad blynyddol a'r cyfrifon;
   - polisïau cyfrifyddu (gan gynnwys unrhyw newidiadau sylweddol) a dyfarniadau cyfrifyddu;
   - y strategaeth archwilio mewnol a'r cynllun ar gyfer y flwyddyn ariannol nesaf;
   - y trefniadau atal twyll;
   - y gofrestr risg weithredol;
   - y gofrestr o weithredoedd tendrau sengl a'r gwariant ar wasanaeth ymgynghorwyr rheoli;
   - braslun o adroddiad blynyddol y Pwyllgor i'r Bwrdd, gan gynnwys y trefniadau i werthuso perfformiad y Pwyllgor.

Cyfarfod 2 (Mehefin):

- yr adroddiad blynyddol archwilio mewnol ar gyfer y flwyddyn ariannol flaenorol, gan gynnwys barn y Pennaeth Archwilio Mewnol;
- y camau i dracio argymhellion archwilio mewnol ac i sicrhau eu bod yn cael eu rhoi ar waith;
- yr adroddiad datgan annibyniaeth blynyddol;
- yr adolygiad blynyddol o'r trefniadau chwythu'r chwiban;
- adroddiad blynyddol y Pwyllgor i'r Bwrdd;
- adroddiad blynyddol a chyfrifon drafft terfynol y flwyddyn ariannol flaenorol;
- adroddiad yr archwilydd allanol i'r rheini sy'n gyfrifol am lywodraethu (ISA260);
- llythyr sylwadau'r archwilydd allanol.

Cyfarfod 3 (Medi):

- y gofrestr risg weithredol;
- canlyniad yr ymarfer dysgu ar ôl cwblhau prosiect yr adroddiad blynyddol a'r cyfrifon;
- adroddiad y swyddog adrodd gwyngalchu arian;
- adroddiad am unrhyw gynigion i dendro ar gyfer swyddogaethau archwilio mewnol ac allanol;
- braslun o'r amserlen i baratoi'r adroddiad blynyddol a'r cyfrifon.

Cyfarfod 4 (Rhagfyr)

- y strategaeth risg a'r trefniadau i reoli risg;
- y camau i dracio argymhellion archwilio mewnol ac i sicrhau eu bod yn cael eu rhoi ar waith.

Atodiad 2

Seiberddiogelwch: rôl y Pwyllgor Archwilio a Sicrwydd Risg

Dyfyniad o Lawlyfr Pwyllgorau Archwilio a Sicrwydd Risg Trysorlys Ei Mawrhydi (daw'r dyfyniad o ddogfen sydd ar gael yn Saesneg yn unig)

1. Audit and risk assurance committees' (ARAC) role is to provide assurance to the Board that the organisation is properly managing its cyber risk including appropriate risk mitigation strategies. This does not necessitate understanding the full detail of the technology involved; ARAC can confirm that the appropriate framework is in place and that continuous monitoring and improvement initiatives are adopted and sustained. It is important to understand the organisation's tolerance for risk and evaluate the risk decisions made by management. Exploring opportunities to share information and to use technology should be guided by the organisation's risk appetite.
2. In particular, to assess the organisation's cyber resilience the ARAC should evaluate whether the organisation has:

   Governance

   - controls in place to prepare for, protect from, detect and respond to cyber-attacks including management of the consequences of a cyber-security incident
   - a means of monitoring the effectiveness of their cyber security controls, including where appropriate, independently testing, reviewing and assuring such controls
   - identified the critical information assets which it wishes to protect against cyberattack and who is responsible for them – whether financial data, operational data, employee data, customer data or intellectual property
   - a way of identifying and agreeing the level of risk of cyber-attack that the organisation is prepared to tolerate for a given information asset; what level of cyber security risk is considered acceptable?
   - an operational risk framework and internal audit plan providing cover across different areas of cyber security, not just focused on IT operations

   Threat Intelligence; Third Party and Supply Chain

   - an understanding of what data is leaving the organisation and its destination, and what associated monitoring activities are in place
   - intelligence processes in place to understand the threat to the organisation's assets including a detailed understanding of which suppliers/partners connect to the organisation and how

- experienced an increase in the number of information security breaches

Structure and Resources

- the right skills and experience in-house to cover all relevant areas
- the right management structure in place, including the Senior Information Risk Owner (SIRO)

Incident Response

- an up-to-date response plan for cyber incidents which has been practiced including actions on lessons learnt

People, Training and Awareness

- training and development programmes to educate the workforce about cyber risks and individual responsibilities; and
- a programme of continuous improvement, or where needed, transformation, to match the changing cyber threat with appropriate performance indicators

3. The ARAC could consider using the organisation's SIRO to provide assurance over these and other issues by:

- getting regular briefs at ARAC meetings from the SIRO, including progress on the maturity of the organisation in information risk and cyber security
- reviewing an annual report from the SIRO as part of the financial year end assurance process and discussing with the SIRO any issues that the ARAC should include in its recommendation for the Governance Statement.

4. A further option for the ARAC is to consider whether one of its members could become a champion on cyber security at the ARAC (and the Board if a member) and support the SIRO.

Archwilio Cymru
24 Heol y Gadeirlan
Caerdydd CF11 9LJ

Ffôn: 029 2032 0500
Ffacs: 029 2032 0600
Ffôn testun: 029 2032 0660

E-bost: post@archwilio.cymru
Gwefan: www.archwilio.cymru

We welcome correspondence and telephone calls in Welsh and English.
Rydym yn croesawu gohebiaeth a galwadau ffôn yn Gymraeg a Saesneg.