Audit and Risk Committee

Tuesday 07th November 2019

09:30 – 12:30

MINUTES

Present:	Douglas Hutchens	Non-Executive Member (Chair)
	Stuart Smith	Non-Executive Member
	Dr Tom Mitchell (by Phone)	Independent Member
Attending:	Lorna Gibbs	Chief Executive (CE) Disclosure Scotland
	Chris McCrone	Head of Finance (DS)
	Gary Devlin	External Audit (EA), Partner Scott-Moncrieff
	[redacted]	Internal Audit (IA) Manager
	[redacted]	Senior Internal Audit (IA) Manager
	Alan Eastwood	Director of Corporate Services
	Laura McCluskey	Director of Disclosure Services
	Stephanie Kerr	Non-Executive Member
	Keith Ross	Non-Executive Member
Other Attendees:	Neill Kemp	Service Owner for item 13
	[redacted]	Independent Accreditor for item 13
Secretary :	[redacted]	Governance Manager
Observer:	[redacted]	Customer Exceptions Team Leader
Apologies:	None	

Welcome and Apologies

1. The Chair welcomed everyone to the meeting. The above apologies were noted.

Declaration of Interests

2. None.

Minutes from Meeting 20th August 2019

3. Amendments were noted to the following:

- Page 2 paragraph 5: GD queried whether he had asked about the EU databases ceasing after Brexit - changed to reflect there was discussion but not assigned to any particular person.
- Page 4 paragraph 15 SS asked if there should be an action regarding providing feedback. (Action now added)
- Paragraph 19 [redacted] asked if it could be reflected that the item was regarding the Transformation Programme Assurance Map and the second sentence reworded to 'no new concerns'.

4. With these amendments, the minutes were agreed as an accurate, true reflection of the meeting. The following actions remain ongoing:

Action/05/July: Resource starting 25/11.
Action/07/July: Doodle poll for 2020 dates sent out 07/11
Action/02/Aug: Agenda item to be tabled at future ARC, Revised Governance for next stage of Transformation paper sent to ARC members 07/11
Action/08/July: Fraud and Bribery discussed at November ARC. Paper to be presented to February ARC detailing figures of certificate fraud from April – December and Customer Engagement Team invited to attend.

Chief Executive Update

5. The CE provided an update on the following:

- LG highlighted the major achievement of coming off BT at the end of September, although the final process felt mildly anticlimactic. Huge praise and thanks to was given to everyone involved.

- December will see us saying goodbye to two of our Non – Executives, Stephanie Kerr and Keith Ross, and a special thanks was given to all the time and effort they have given to the Disclosure Scotland Board.
  Our recent recruitment exercise resulted in 30 applications and 8 interviews with three appointments being made.
  [redacted] will be bringing Governance expertise, [redacted] Change Management experience and finally [redacted] brings Human Rights and Equality. All three will be attending the Board in December.

- Audit Scotland have confirmed that there will be a Section 22 issued in relation to the Transformation Programme. The draft was expected by the end of next week. LG is meeting with Paul Johnston, Michael Chalmers and Colin Cook on Monday to discuss. Expected publication on Tuesday 17th December.

- It is expected that the Auditor General will attend the PAPLS Committee after January 16th in respect of the Section 22, but, hopefully not the same date as the

first stage of Disclosure Bill. The S.22 should mirror Scott-Moncrieff report. There may be media coverage beforehand but media lines being developed.

- SS advised that he was pleased that we had commissioned someone to help with the media lines and stressed how important it is to prepare and offered the ARC's help with this.

- LG explained that DS was experiencing some challenges as regards the SLA timescales not fully being met. This was not a direct factor of PASS but a number of different factors coming together at the one time. Measures have been put in place and include a reduced hours helpline and secondment of staff from other areas to Disclosure Services to help reduce the workload. Positive changes are being made and the situation will be monitored closely over the coming weeks.

Internal Audit Progress Report

6. It was noted that Internal Audit are on track to deliver on the 2019/20 plan and will be on time. EY are an IA sourcing partner and will be looking after the Common Agricultural Policy (CAP) work and providing additional resource/skills as and when required. They will not be working directly on DS assignments unless there is a requirement for specialist skills not already within the Directorate of Internal Audit and Assurance (DIAA) e.g. Cyber security audits.

7. The Governance and Risk Audit has started and IA has observed at a number of meetings already with the dates expanded to enable attendance at all relevant meetings. They have been pleased with the assistance they have been given from DS staff.

8. The financial modelling follow up audit has been completed but DS resource issues have meant that the GDPR review has had to be postponed. A new resource will be available from the 25th November.

9. SS was pleased that EY had been appointed as IA recognise that they can't be experts in all fields. TM agreed that it was good to identify skills gaps and take steps to address.

10. Internal Audit are looking for suggestions for inclusion for the new plan. It was important to get the right assurance. If ARC members have suggestions, they should discuss with DH who will be liaising with IA over the next few weeks.

Quarterly Review of Fraud and Bribery – how external Fraud is reported to the ARC

11. There have been no actual, or attempted, incidents of Fraud or Bribery.
Discussion took place around external fraud and how this is reported to the ARC. AE spoke about instances of Certificate fraud as reported by the Customer Engagement Team. It was agreed to invite someone from the Customer Engagement along to February ARC to explain how they record the instances of fraud and what action they take. A paper will also be provided to show figures from April – December.

Action/01/Nov: CET to be invited to February ARC.

Audit Recommendation Tracker

12. The Director of Corporate Services provided information on the Audit Tracker and asked the ARC to ratify the closing of 11 recommendations.

The Committee were happy to sign all off.

TM expressed concern that GDPR risks have red status but is sitting at low risk and with documentation and measures still not in place, asked how breaches and issues can be dealt with consistently. AE stated that measures are in place, all staff were aware of the process and that each breach was being looked at on a case by case basis. The gap in internal resources which was stopping some of the documentation being implemented has now been filled with the post holder starting on the 25th November.

LMcC indicated that training has been put in place but is not currently being tracked and managed. The Committee requested that more narrative added to the tracker to reflect all the measures that were in place.

Action/02/Nov: CGT to obtain more narrative for next ARC.

Deep Dive into Spending Review (20/21+)

13. DH thanked AE and SS for producing the paper and extended invite to SK and KR to contribute fully to the discussion.

AE provided the background to the paper and talked through the paper.

14. AE advised the committee that he would circulate an Income Report, submitted to the October Board to the committee for information.

Action/03/Nov: AE to circulate Income Report to committee.

15. The Committee agreed that the paper was a good start but felt it would be useful to 'stress test' the figures and scenarios provided. They felt that it should lay out the assumptions and look at optimistic, pessimist and somewhere in the middle situations whilst drawing out the risks.

16. Further discussion took place around staffing levels, efficiency savings and the risks. It was agreed more in depth paper to be brought to both the January Board and the February ARC and for sufficient time to be allocated to discuss this in full.

Action/04/Nov: AE and SS to produce a paper with high level tables and draw out more information to be discussed at Jan Board and Feb ARC.

Financial Performance (19/20)

17. Discussion took place around the original agreed budget (paragraph 14) and the knowledge that this would be an indicative budget, as there would be a need to request more funding. It was noted that an explicit narrative was needed as someone not aware of this position and background will think that we are significantly over budget, not realising that budgets can be moved and adjusted at the end of year.

18. It was noted in paragraph 15 that DS has made a conscious decision, based on the type of work that they are doing, to classify some programme contractors as capital expenditure. The cost of these contractors has been included in the capital forecast presented.

19. The Director of Children and Families has agreed that capital funds are available until the end of December 2019. If capital funding is not available in quarter 4 then further work planned in this quarter may not be able to continue.

20. The workarounds have been costed at c. £3m (19/20 only) and although they will be in place for a while, each business area is being looked at to see how they can be optimised.

BT Security incident

21. Supplier gave device to the wrong courier - DHL instead of UPS so device was sent to a DL location in Bristol and not to where intended. Device is an appliance for transferring data to the supplier from clients. Supplier located the device and was directed to correct address.

22. Device had multiple layers of encryption and tamper seals and these were all intact. Supplier has changed their security process for courier collection.

Quarterly review of information breaches

23. DPO was unable to attend the meeting so AE talked through the report. He advised the ARC that a Continuous Improvement group had been set up by the Senior Governance Manager which will be looking at the issue of breaches. They will look at different processes and try to mitigate the risks in different areas.

24. No cases have been reported to the ICO after discussion between DPO and the ICO. A number of investigations have taken place and the nature of the breaches are such that no personal issues have arisen.

25. Staff awareness of the issue has increased and they now know what they need to report and when they need to report which may be a reason why this number has increased.

26. Different areas are looking at integrating data handling into staff objectives to ensure greater staff awareness.

27. Disclosure Services are seeing a significant increase in breaches through the new mailroom processes and area is being looked at to try and mitigate risks.

Quarterly review Risk Register

28. No new risks have been added to or escalated from local risk registers to the Corporate Risk Register.

29. Discussion took place regarding the issue of data breaches and the committee were advised that a Deep Dive would be carried out at the Performance Team meeting. A Lean Group has also been established and will look at processes within DS, starting with some of the areas that data breaches occur most frequently.

30. The committee agreed that the risk register should be discussed more often and in more depth at the Board meetings.

31. The current workarounds were discussed and it was commented that although the requirement and risk related to them is articulated within another risk, they should perhaps be contained within their own risk. It was felt that the risk was more specific to certain areas and AE volunteered to speak to GH about how the risk should be highlighted on local registers.

    Action/05/Nov: AE to discuss with GH how to highlight workarounds risk on local registers.

Cyber Security

32. NK and [redacted] joined the discussion.

33. [redacted] provided some background to the organisation and to the aspects he had covered in his report. He explained that along with Cyber Security for the organisation, he also looked at physical security and reassured the ARC that the physical security in both the main building and in the Hub was good.

34. He noted that we have been a ground breaking organisation, being the first to store things on the cloud, which other organisations had been considering but hadn't done yet.

35. He advised that resourcing is an issue within the organisation and we are struggling to find the right people that we need to get things to drive this forward.

36. The ARC thanked them for the paper but felt that it would be better for the organisation to look at the different vulnerabilities and categorise them. From an audit point of view DS needs to identify different areas of vulnerabilities as there were 244,000 last year on pen tests. The ARC felt they didn't know what kind of systems DS use, what kind of training was carried out and felt that it would be useful to present a paper on a regular basis to the ARC which could cover a variety of different issues in this regard.

37. The biggest risk for the organisation was felt to be human error or human misconduct rather than cyber and our systems are pretty resilient. Every transaction completed is logged which [redacted] takes some comfort in.

38. TM offered his services to become part of the working group being set up. [redacted] was asked if he had been in touch with [redacted], and [redacted] advised he would be happy to revisit Scottish Cyber Resilience.

Terms of Reference

39. The committee discussed the Terms of Reference and were happy with the changes noted. SS commented that the calendar of business would usually be attached to the ToR but as this has still to be finalised it will be brought to the next ARC meeting.

Action/06/Nov: Calendar of Business 2020 to be discussed at Feb ARC

40. Two reports were discussed at the Board – the Income report and the Revised Governance paper. AE advised that these papers would be sent to the ARC members following the meeting.

Action/07/Nov: Revised Governance paper and Income Report to be sent to ARC members

AOB

No other items were discussed.

Next Meeting 26th February 2019, 10:00 – 12:30, Meeting Room 1a.

Action	Responsible	Due by	Status
Action/05/July: GDPR6 to be confirmed with Data Protection Officer.	Data Protection Officer	ASAP	DPO confirmed that the form has been drafted. Guidance will take longer as department lacking in resource and audit tracker will be updated to reflect. New B2 Resource starting on 25th November **Action Closed**
Action/07/July: CGT to look at times of future meetings and adjust ones which require pre-meetings accordingly	Secretariat / CGT	ASAP	Doodle Poll for 2020 dates sent out 07/11. Later start for all meetings to accommodate pre- meetings **Action Closed**
Action/08/July: Fraud and Bribery - to discuss external Fraud at next ARC meeting.	AE	7th November ARC	External Fraud discussed at 07/11. Agreed that sweep would incorporate extra parts to take external fraud into consideration. Rep from Customer Engagement to attend February ARC. **Action Closed** .
Action/01/Aug: Deep Dive into next steps of Transformation Programme and associated risks	Chair	TBC	Agenda item for ARC postponed to be tabled for future meeting
Action/01/Nov: CET to be invited to February ARC to discuss Certificate Fraud.	CGT	February ARC	CET member accepted invite to attend February ARC meeting 26/02/20: Meeting overran so CET will be invited to present at May meeting **Action ongoing**

Action/02/Nov: CGT to obtain more narrative for next ARC regarding GDPR recommendations.	CGT	ASAP	More narrative added and re-issued to ARC members **Action Closed**
Action/03/Nov: AE to circulate Income Report to committee.	AE	7th November 2019	Papers added to the ARC Connect file and emailed members to advise available. **Action Closed**
Action/04/Nov: AE and SS to produce a paper with high level tables and draw out more information to be discussed at Jan Board and Feb ARC.	AE and SS	26th February (ARC)	Agenda item for January Board. Paper presented at January Board, still to be presented at Feb ARC **Action Ongoing**
Action/05/Nov: AE to discuss with GH how to highlight workarounds risk on local registers.	AE	ASAP	Discussed at DS Corporate Risk Review Group. Innovation Risk 1 has been added to the Corporate Register to ensure the required Corporate focus. **Action Closed**
Action/06/Nov: Calendar of Business for 2020 to be added to the agenda for February ARC	Chair/CGT	February meeting	Agenda Item 16 on February agenda. **Action Closed**
Action/07/Nov: Transformation Governance paper and Income Report to be sent to ARC members.	CGT	7th November 2019	Papers added to the ARC Connect file and emailed members to advise available. **Action Closed**