



Information Security Strictly Confidential

Information Security (IS) Committee
05th June 2014 at 10:30 in Room 501 - 148 Old St

Attendees	Julie George - Head of Information Security & Assurance – Chair Alan Simpson – ISAG Compliance Support – Scribe Malcolm Zack – Head of Internal Audit Kevin Seller - Head of Government Innovations Programme Toni Sless - representing John Scott - Head of Security Andy Garner – Head of Managed Services Roger Gale – Head of Crown Network Nick Fox – Senior Manager, Customer Management Adnan Killedar – Risk & Compliance Rod Ismay – Head of Finance (dial in)	
Apologies	Belinda Crowe – Compliance Partner Michelle Ranger – HR Business Partner Piero D’Agostino representing Head of Legal Dave Hulbert – Head of IT Services Dave Mason – Head of Risk & Compliance Elena R Nistor – IT Audits Jonathan Hill - Head of Risk, Banking Regulation and Strategy, Financial Services Peter Goodman – Head of Finance Operations	
Agenda Item	Agenda Points	Action
1	<u>Introductions</u> Julie George welcomed everybody and reminded about the importance to attend this Committee and also the requirement to send a deputy if invitees unable to attend.	All
2	<u>Actions from previous meetings</u> The minutes from the previous meeting were approved. Previous actions covered separately as below.	JG
3	<u>Information Security Policies</u> <ul style="list-style-type: none"> As per the previous ISC meeting JG noted, again, that the AUP (Acceptable Use Policy) has still not been signed off, A 'Noting' paper has been sent to Risk & Compliance to facilitate the acceptance of the risk. BYOD (Bring Your Own Device) policy is in planning stage by ISAG. At the recent Risk & Compliance meeting ISAG were asked to provide an acceptable option that is both in line with the policy and acceptable to the Board. This has the backing of Paula Vennells. 	JG
4	<u>Input from Working Party</u> No issues to escalate at this time. Previous issues, noted as escalation items, covered under 'Input from JV/Supplier ISMF's have been resolved.	JG
5	<u>Input from JV / Supplier ISMFs</u> JG noted that Atos will be undertaking the management of certain ISMFs going forward, once information flow between the two organisations has been agreed.	JG
6	<u>Current Audits</u>	

Information Security Strictly Confidential

	<p>JG explained that:</p> <ol style="list-style-type: none"> 1. POL ISAG is preparing for this year's PCI DSS audit which is scheduled to take place July/August with the reporting and certification stage in October. 2. ISO27000 audits will also be undertaken in a selection of branches over the coming months in relation to Government Services. 	
7	<p><u>Incidents</u></p> <ul style="list-style-type: none"> • Current list of open incidents was discussed at this meeting and 4 out of the 10 open incidents requested for closure were agreed at this meeting. 	
8	<p><u>Regulators submissions to the authorities</u></p> <ol style="list-style-type: none"> 1. Nothing to report at the time of this meeting 	JH was unable to attend but nothing had been sent to the committee for notification
9	<p><u>Any Other Business</u></p> <ol style="list-style-type: none"> 1. AUP – covered under section 3 – Information Security policies 2. SharePoint issue re new Business Travel Policy rates for hotels spread sheet. This was raised by MZ as a security issue due to the Share Point document allowing users to edit the listed rates. Noted as possibly an isolated incident and whilst not being business critical it does raise concerns around the security of all Share Point sites and the content. Paul Swanton confirmed the correct level of access is on all the things we have but is only a small percentage of what is out there. JG suggested that this be further investigated by the ISWP re suitable solution. 3. RG raised the question as to whether Royal Mail employees still have access to POL printers on the network. To be raised in the ISWP. 4. BIA/PIAs – (Business Impact and Privacy Impact – Assessments) – JG noted that these are fairly new for the Post Office and will highlight any criticalities of the systems as it is evident that the business is not fully aware of what we have and who has responsibility , with regards to assets, information, systems etc.. The first stage will be to engage with ExCo and then this will be extended out to team members. This exercise will provide better understanding of priorities and responsibilities and the BIA will highlight associated risks. The initial stage will commence next week, with the first report produced around early July – for presentation to the Board. 5. Rod Ismay broached the subject of risks around use of Social media by employees. JG noted that all are subject to the adherence to the contents of POL policies and should be aware of the consequences. RI noted the use of Twitter being used to raise concerns and issues, both negative and positive. JG suggested this be raised in the ISWP for progression. 6. AS to provide glossary of acronyms for ISC minutes to facilitate better understanding of those terms used. 7. RI noted the number of meetings that use projectors to provide information, some of which is commercially sensitive which is visible to those from outside the building via open/unshielded windows. To be raised via the ISWP. 	

Information Security Strictly Confidential

Glossary	ISC – Information Security Committee ISWP – Information Security Working Party BYOD – Bring Your Own Device ISAG – Information Security & Assurance Group ISMF – Information Security Management Forum PCI DSS – Payment Card Industry – Data Security Standard AUP – Acceptable Use Policy BIA – Business Impact Assessment PIA – Privacy Impact Assessment FOoG – Front Office of Government DP – Data Protection DPA – Data Protection Act	
Next Meetings	July 04th Room 506, 148 Old Street - 10:30 – 12:00 August 07th Room 202, 148 Old St – 09:30 – 11:00 September 04th, Room 311, 148 Old St. 09:30 – 11:00	

Actions from previous meetings:

Update on outstanding actions:		
<p>1. ACTION (250713): Progress ownership of the Home Office Clearing (currently with the project) with HR or Security. <i>The aspiration is to transfer to HR, but they need headcount. HR has taken external advice.</i></p> <p>03 03 14 – owner in HR to be found, security clearances on-going, reassign to Jonathan Hill</p> <p>08 05 14 – John Scott's Security team still undertake Security Check Clearances on behalf of the business and FOoG, however, they are awaiting an update from our HR Business Manager as to progress. These were previously managed by Group. Discussions are on-going with Michelle Ranger and escalated to Joe Connor. TS noted that this was an item for discussion in today's SLT meeting. TS took an action to provide an update following today's SLT.</p> <p>05 06 14 – TS confirmed that this action point is still 'on-going' and although it has been escalated it is dependent on the outcome of the current Security Team restructure JG noted that this has been highlighted to Lesley Sewell via ExCo.</p>		KS – reassign d TS
<p>2. ACTION (250713): The Information Security e-learning non-completions will now be escalated to their line managers. <i>Will be progressed by Claire Davies.</i></p> <p>03 03 14 – Claire Davies still chasing – on-going.</p> <p>08 05 14 – Noted that some colleagues did not receive the initial cascade so will account for a certain percentage of failings. Katie Barber is aware of those non-receivers and will take an action to send list of all Finance team non-completions to Jonathan Hill.</p> <p>05 06 14 – No update available at time of this meeting. AS to chase up with Katie Barber.</p> <p style="padding-left: 40px;"><i>Lack of access for contractors is also being investigated by HR</i></p>		JG
<p>3. ACTION (081013): The P6 Requests that will need to be transitioned to the Service Desk. <i>This is being progressed by Dave King.</i></p> <p>03 03 14 – On-going, will be transferred to Service Desk eventually.</p> <p>08 05 14 – Service Desk not accepting P6 requests as yet but there is an interim measure in place currently. JH raised concerns regarding customers' information being given to Service Desks in Manila despite assurances to the contrary. There is no plan to move services to Manila and no programme to share as not available. Support for Horizon ceases from June 2014.</p> <p>05 06 14 – Update to be provided for next ISC meeting.</p>		JG reassigne d to BH

Information Security Strictly Confidential

<p>4. ACTION (071113): Investigate how business and Grapevine incidents can be aligned with the SDM12 IT incidents. 03 03 14 – On-going 08 05 14 – No progression on this one. Tender process underway so not a priority. BH to speak with Dave Pardoe in POL Security to discuss further. 05 06 14 – No further progress. AS to chase for update from BH and ensure that Andy Garner copied in on any progress. AG also queried if the correct product had been purchased and whether any due diligence had been attached to the purchase of the new Incident Management System tool.</p>	
<p>Closed/Completed Action Points from previous meeting:</p> <p>ACTION (250713): Belinda suggested that some of these documents should potentially be published on the external website (linked to FOI). This will be discussed with Mark Davies. 03 03 14 – No update available at time of this meeting. On-going. 08 05 14 - No update available at time of this meeting, suggestion is that we ask for closure on this since it is an FOI suggestion and we don't deal with FOI 15 05 14 – Update received from BC stating that it was not possible to clear this AP as, previously, it was pending an ExCo decision on the Scheme. This decision has now been made and Mike Granville is progressing this work. MG has been informed that BC is providing further input and also that there will be a need to factor in further liaison with this Group should he wish to publish relevant security policies. BC agreed closure on that basis.</p> <p>ACTION (071113): The Committee agreed that the analysis of the 14 key system interfaces will need to complete sooner (if needed with prioritisation from Lesley Sewell), which will be explained to Kevin. 03 03 14 – analysis of 14 key system interfaces – needs clarification. On-going. 08 05 14 – Commencing BIA/PIA's across the business with rollout expected from June. 05 06 14 – Updated under A.O.B. AP Closed.</p>	<p style="text-align: center;">BC</p>