Queen Mary
UNIVERSITY OF LONDON

Matters Arising

Outcome requested:	Audit and Risk Committee is asked to **note** the matters arising from the minutes of the meetings held on 10 November and 01 October 2020.
Executive Summary:	N/A
QMUL Strategy: strategic aim reference and sub-strategies	The effective management of the Queen Mary's governance arrangements underpins the ability to achieve the strategic aims.
Internal/External regulatory/statutory reference points:	N/A
Strategic Risks:	N/A
Equality Impact Assessment:	Not required
Subject to prior and onward consideration by:	Considered by the Committee only.
Confidential paper under FOIA/DPA	No
Timing:	N/A
Author:	Nadine Lewycky, Assistant Registrar (Governance)
Date:	23 February 2021
Senior Management/External Sponsor:	David Willis, Chair of Audit and Risk Committee

Actions from meeting of: 10 November 2020

Minute no.	Action	Person responsible	Progress
2020.041[a]	**Audit and Risk Committee Annual Report 2019–20 draft 2 [ARC2020/32]** The Committee had no substantive comments on the draft and any minor points would be shared with the Committee Secretary by email. A finalised draft would be circulated to the Committee for approval following the meeting.	Committee Members; Secretary	A finalised draft was circulated after the meeting which was approved before submission to Council.

Actions from meeting of: 01 October 2020

Minute no.	Action	Person responsible	Progress
2020.003[a]	**Matters arising [ARC2020/02]** *Cyber security* The criteria for reporting on cyber security would be finalised and reported to the next meeting.	Chief Governance Officer and University Secretary	**Reporting to Audit and Risk Committee** It is recommended that reporting to Audit and Risk Committee should be on the basis of a retrospective bi-annual written report. This would also cover wider metrics around business continuity, incident response timescales and impact on service users. In terms of real-time reporting of incidents, it is recommended that reporting to A&RC should be on the following criteria: • A systemic issue affecting the integrity of data which could lead to fraud or an inability to provide reliable data to our regulators; • A material breach of personal data that could foreseeably lead to a penalty; • Anything that might have reputational impact nationally; • Anything that might result in a material financial loss; and • Anything that prevents people across the University from being able to work for more than a day.