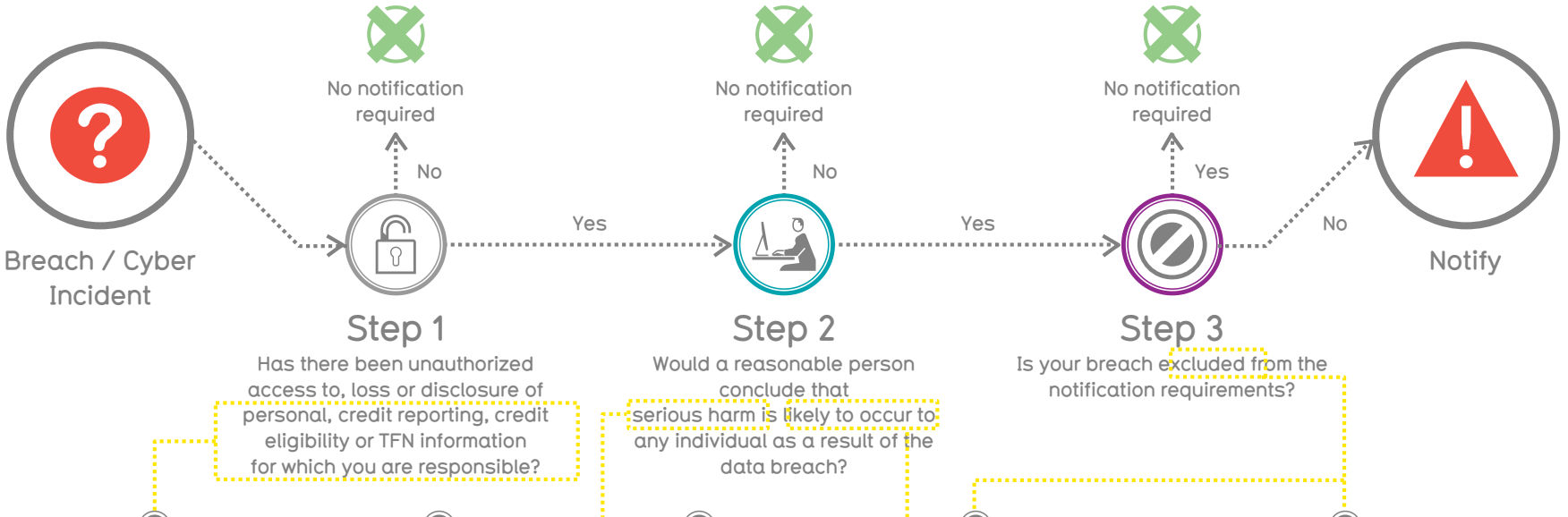
Data Breach Notification Guide

From 22 February 2018 the Privacy Act imposes a mandatory requirement to notify all "eligible data breaches" (MDBN).

Any agencies or entities covered by the provisions must, as soon as is practicable, notify the OAIC and all affected individuals if a "reasonable person" would believe that any of those individuals is likely to suffer "serious harm" as a result of that data breach.

EY
Building a better working world

Do you need to notify?



Information covered	Serious harm	Likely to occur	Exclusions	Practicalities
It is important to note that MDBN obligations apply more widely than privacy obligations under the APPs: MDBN catches any person (ie everyone) in respect of TFN information, as well as APP entities in respect of personal information, credit reporting bodies in respect of credit reporting information and credit providers in respect of credit eligibility information.	Whether harm is 'serious' depends on the type of information, the individual and the surrounding context. Serious harm could involve physical, psychological, reputational and/or financial harm. Matters to consider in determining whether a reasonable person would consider the seriousness of the harm are included in law.	The OAIC has previously considered 'likely' as, 'the chance of the harm occurring being more probable than not probable.' The likelihood may be affected by the anticipated intentions of the persons who have acquired the data.	1. Where 'remedial action' has been taken such that any harm resulting from the data breach will no longer be serious or harm is now unlikely to arise. 2. Enforcement related activities / Commonwealth Secrecy Provisions / Privacy Commissioner declarations. 3. Where one entity in the 'chain' has already notified the data breach.	To benefit from the limited exemptions from mandatory notification (eg by eliminating any risk of serious harm occurring to any individual and before any serious harm actually occurs), the privacy management and compliance of the relevant agency or covered entity will need to be mature/best practice. In any event, all agencies will need to implement a privacy management plan from 1 July 2018 in order to comply with Privacy (Australian Public Service – Governance) APP Code (APS Privacy Code), assuming the current draft is adopted as is.