A)1. “The department monitors risks that may impact the achievement of strategic objectives according to the level of appetite. The department has the lowest appetite for risks associated with:

- safety of children and students;
- workplace health and safety of its staff and the community;
- security of confidential and personal information held by the department; and
- fraud and corruption.

As its foundation, the department has a core requirement to comply with its legislative obligations in its pursuit of quality outcomes for children, students and the community.

The department is willing to accept a higher level of risk when pursuing innovation and opportunities that further its strategic objectives to give all children a great start, engage young people in learning and creating safe, fair and productive workplaces and communities….”

This Risk appetite statement comes from Queensland Government’s Department of Education. [Link: https://ppr.qed.qld.gov.au/attachment/risk-appetite-statement-and-categories.pdf ]

2) I think it is a good example of risk appetite as it follows Provititi’s risk appetite framework by:

- listing areas for which they will take minimum risk
- stating their willingness to accept higher risk in certain area, if it furthers their strategic objectives
- providing a table with the strategic objectives and ranking them in terms of low to high appetite, alongside providing a legend to clarify what it means by low or high *(see page 2 and 3 of the document)*

B)1. According to Peltier, in any company, the Senior management, Chief information security officer, System and Information owner, Business Manager and Information Security Administrator should be responsible for risk analysis and management. That’s because as a whole, these roles determine not only the appropriate resources (budget) allocated to fulfill the mission requirements (and business objectives) efficiently and effectively, but also ensure that proper controls are in place to fulfill the Confidentiality, Availability and Integrity of the information that they own. In the eTricity case, Peltier’s roles’ conditions are fulfilled by Owners Brad and Angelique (who can override board’s decision), CFO Josh (who determines their market stance), Board of directors, Business Managers and “subbies” (who mainly has access to and controls the business and customer information), Info System Manager Alain (who focuses on overall IT security) and the Chief data officer Jock and his team of Database administrators and programmers (who focus on data analytic and processing information), HR Manager Rebecca (who handles employee payment data), Customer Service Manager Theresa (who handles customer data), design engineers (who handle data regarding their prototypes’ design), Chief Engineer Felix (who handles supplier data) and the Accounts reconciliation officer Sally (who handles invoicing data).

2. The 6 steps of Peltier's Risk Analysis Process:

- Define assets on which we will perform risk analysis
- Identify threats
- Determine likelihood of threat occurring
- Determine impact of the threat
- Identify controls to reduce risk to acceptable level or eliminate it
- Document the risk analysis in a report format

3. In Peltier's paper, the Enterprise risk analysis process is a form of assurance or proof that ensures that the company is indeed performing its due diligence.