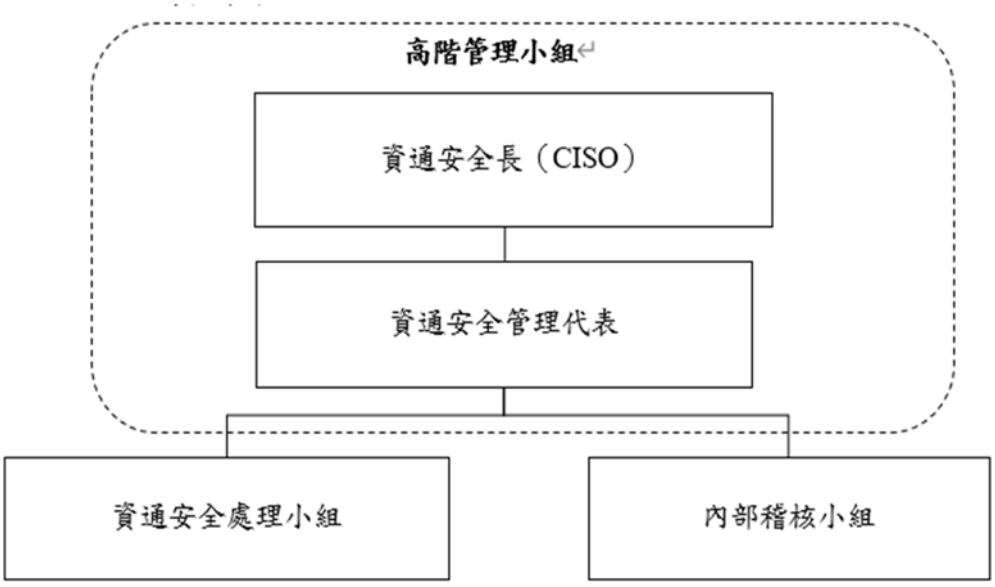
宇智網通已成立資通安全組織架構，並設置完善、嚴謹的資通安全管理流程，說明如下：

(一) 資通安全風險管理架構、資通安全政策、具體管理方案及投入資通安全管理之資源：

1. 資通安全風險管理架構



【註】資通安全長：由本計畫「總經理」擔任、資通安全管理代表：由「營運處主管」擔任。

高階管理小組：由「資通安全長」、「資通安全管理代表」及「資通安全顧問」所組成。

本公司因應 ISO 27001 資訊安全管理標準之要求，特制訂本政策作為整體 ISMS 之建置開發、實施操作、監控審查及持續改善之規範，並依據本公司業務活動與風險，以建立資通安全管理政策及管理目標。

同時沿用國際標準組織（ISO）所訂定之持續改善 P.D.C.A.循環流程管理模式，整合及強化資通安全管理體系。

2. 資通安全政策

為了促使本公司 ISMS 能貫徹執行、有效運作、監督管理、持續進行，包括以下三方面，說明如下:

(1) 制度規範:本公司內部制定多項資安規範與制度，本政策旨在讓同仁於日常工作時有一明確指導原則，所有同仁皆有義務積極參與推動資通安全管理政策,每年定期檢視相關制度是否符合營運環境變遷,並依需求適時調整，每年定期執行內部稽核、會計師資訊稽查、ISO 外部稽核，以強化本公司機密之作業管理。

(2)系統防護:本公司為防範各種內外部資安威脅，除採用多層式網路架構設計外，更建置各式資安防護系統，貫徹執行資通安全作業，確保業務資料之機密性、完整性及可用性，免於因外在之威脅或內部人員不當的管理，遭受洩密、破壞或遺失等風險。

(3)人員訓練:為確保所有同仁皆有能力執行所要求之工作與符合各項安全要求，藉由各種資安教育訓練，提升內部同仁的資安知識與專業能力。

3. 資通安全具體管理方案

具體管理方案，分別以下列四方面說明:

(1)權限管理:人員帳號權限/密碼，皆定期盤點及定時強迫更換密碼。

(2)存取控制:人員帳號權限皆由 AD server / ERP / PLM，依據不同工作職掌， 管理系統存取權限。

(3)外部威脅:使用防火牆攔阻外部惡意攻擊及防毒軟體進行公司內、外部病毒、惡意程式等偵測。

(4)系統可用性:建置 VMWarevm 虛擬機以及 Veem 即時備援系統，並定期災害復原演練。

4. 投入資通安全管理之資源

本公司不定期宣導資安案例，並不定期更新軟、硬體資安防護設備及維護合約簽定，以確保各項防護維持在最新狀態。

(二) 最近年度及截止年報刊印日止，因重大資安通安全事件所遭受之損失、可能影響及因應措施:無此情形