



A. Background Information

Information of Critical Infrastructure Operator ("CI Operator")

Full Name:

B. Change Details

1) Type of Material Changes †

- | | |
|--|--------------------------|
| Platform migration | Server virtualisation |
| Changes to the computing platform or hardware | Application re-design |
| Major version upgrade of a core component (e.g. database) | Significant code changes |
| Integration with or change in interdependency on external systems or networks | |
| Changes to the underlying infrastructure that supports the critical computer systems ("CCS") | |
| Any system modification that fundamentally alters the characteristics or nature of the CCS | |
| Substantial changes in CCS components maintained by cloud service suppliers that the CI Operator becomes aware of | |
| Change of mission or major functions that alters the system's operational scope, intended purpose or requirements in security, resource or functions | |
| Others (please specify): | |

*Please refer to section 22 of the Protection of Critical Infrastructures (Computer Systems) Ordinance for meaning of "material changes".

2) Change Details with Timeframe †

3) Deployment Date (dd/mm/yyyy)

*Please refer to section 6.1 of the Code of Practice for details.

*All the changes should be endorsed and processed in accordance with the change management process defined in the computer-system security management plan.

4) Description of the Effect (on the computer-system security risk of the CCS(s) or risk to carrying out the core function of the CI after the deployment of the material change(s))

*Please include the relevant computer-system security risk assessment documentation in the submission of this form.

5) Updated System Documentation

*Please list the documentations attached with this form.

C. Reporting Entity Information

Name:	Post Title:
Office & Mobile Contact:	Email Address:
Form Submission Date (dd/mm/yyyy):	

Personal Information Collection Statement: The personal information provided will be used for the purpose of exercising the powers and duties vested in the Commissioner of Critical Infrastructure (Computer-system Security) ("the Commissioner") or the designated authority specified in column 2 of Part 2 of Schedule 2 of the Protection of Critical Infrastructures (Computer Systems) Ordinance ("the Ordinance"), collectively known as the regulating authority. The personnel information will be retained by the regulating authority for an appropriate period of time necessary for the fulfilment of the relevant purposes or as required by the Ordinance. The regulating authority may disclose the personal information to the parties permitted by section 57(3) of the Ordinance. The data subject or relevant persons as defined in section 2 or 17A of the Personal Data (Privacy) Ordinance ("the PDPO") have a right of access and correction with respect to personal information as provided for in sections 18 and 22 and Principle 6 of Schedule 1 of the PDPO. The right of access includes the right to obtain a copy of the personal information provided in this form. Enquiries concerning the personal information collected by means of this form, including access and corrections, should be addressed to the Commissioner (email: protection_ci@sb.gov.hk) or the designated authority concerned.