Overview of regulatory requirements, guidance and approaches to cyber security[1]

Regulator	Content/*Observations*
Australian Securities & Investments Commission (ASIC)	• Australian financial services licensees are required to maintain proper risk management processes pursuant to s912A(h) of the Corporations Act (depending on their operations, this will usually include processes to deal with cyber risks) • Recently (03/2015) published Report 429 on "Cyber resilience: health check": includes a health check list (page 8-14) and relevant legal and compliance requirements for different types of regulated entities (Section D and Appendix 2)
Autorité des marchés financiers (Québec, Canada)	• Cyber security implicitly covered in Part 11 (internal controls and systems) of Regulation 31-103 respecting Registration Requirements, Exemptions and Ongoing Registrant Obligations (c. V-1.1, r. 10) • The Canadian Securities Administrators/Autorité canadiennes en valeurs mobilières CSA/ACVM also published two Staff Notices: CSA Staff Notice 11-326 Cyber Security and CSA Staff Notice 11-321 *Business Continuity Planning – Industry Testing Exercise*
Bank of England Financial Stability Report (07/ 2015)	• Section on Cyber Risk (p.31-33): Addresses concerns about disruption of critical functions in the financial sector • Firms should focus on vulnerability testing, recovery capabilities (to resume vital services quickly) and effective governance.
FCA Handbook	• SYSC 3 Systems and Controls: focus on establishing and maintaining (1) systems and controls appropriate to the firm's business and (2) risk-centric governance arrangements • SYSC 6.3 Financial Crime: mostly focussed on money laundering and where firms could be used to further financial crime • Principle 3: Management and Control: "…reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems" • Principle 11: Relations with regulators/disclosure: "... deal with regulators in an open and cooperative way" and disclosure to regulators; SUP 15 may imply a requirement to notify the FCA or PRA of serious cyber security incidents (e.g. SUP 15.3.1 Matters having serious regulatory impact) *Issues relating to cyber security **implicitly** addressed in the FCA Handbook in a principle-based fashion; no dedicated cyber security section.*
FCA "One-minute guides": Data security	• Focus on customer data safety, including governance, compliance monitoring, systems and control, physical safety, vetting of staff (e.g., credit checks, criminal record checks), due diligence of third party service providers, staff awareness, disposal of data (also see the Data Security Factsheet) *Six page summary of key responsibilities and action items*

[1] In addition to the dedicated approaches of financial regulators, a number of national governments have conducted cyber-attack simulations and surveys on cyber security preparedness. Examples are included in Appendix C.

Regulator	Content/*Observations*
Monetary Authority of Singapore (MAS): Technology Risk Management Guidelines and Notice on Technology Risk Management	*Guidelines* • Focus on technology risk management principles and best practices that cover areas such as system security and the protection of customer data and transactions • Section 9 "operational infrastructure security management" covers measures to address the risks of cyber-attacks *Notice* • Sets out requirements to notify MAS of serious security breaches of critical systems *The government also is setting up a dedicated Cyber Security Agency (CSA) under the Prime Minister's office, building capabilities and collaborating with the private sector*
National Futures Association (NFA) Self-Examination Questionnaire (02/2016)	• Cyber security questions were added to the NFA Self-Examination Questionnaire • This section is designed to help member firms comply with NFA's Information Systems Security Programs (ISSP) rules and interpretations which came into effect on 1 March 2016
SEC OCIE Examination Priorities for 2016 (01/2016)	• In the area of cybersecurity, the 2016 examination priorities include testing and assessments of firms' implementation of procedures and controls *Follow on from previous initiative (please see line below)*
SEC OCIE National Exam Program Risk Alert (09/2015)	• Additional information on the OCIE's second round of cyber security examinations, which will involve more testing of the firms controls • Particular focus on protection of client information and cyber security-related basic controls (governance and risk assessment, access rights and control, data loss prevention, vendor management, training, incident response) • The appendix contains a sample list of materials the OCIE may review *Follow on from previous guidance (please see line below: SEC guidance April 2015)*
SEC Division of Investment Management Cyber Security Guidance (04/2015)	• Conduct periodic assessment of (1) nature, sensitivity and location of information, … (2) threats to the IT systems, (3) security controls/processes, (4) impact if systems are compromised, (5) effectiveness of governance structure • Create strategy to prevent and detect threats • Written policies/procedures/training *High level guidance*
SEC OCIE Cyber Security Examination Sweep Summary (02/2015) [2]	• Summary of examination findings of 57 registered broker-dealers and 49 registered investment advisers, focusing on information security policies, business continuity plans, use of external standards (e.g. NIST, ISO or FFIEC frameworks), periodic risk assessments, approach to service providers/vendors, etc. *Provides a good understanding of the OCIE's examination priorities; the program is still being developed/enhanced*

[2] SEC OCIE: Securities and Exchange Commission Office for Compliance Inspections and Examinations

Regulator	Content/*Observations*
National Conference of State Legislatures (US)	Overview of security breach notification laws (legislation requiring entities to notify individuals of security breaches of information involving personally identifiable information)
Securities and Futures Commission of Hong Kong	• Part IV (Information Management) of "Management, Supervision and Internal Control Guidelines for Persons Licensed by or Registered with the Securities and Futures Commission": policies and procedures are required to be established to ensure integrity, security, availability, reliability and completeness of all information, including documentation and electronically stored data, relevant to the firm's business operation. • Para 18.5 (Adequacy of System) of "Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission": also requires that a licensed or registered person should ensure the integrity of the electronic trading system it uses or provides to clients, as may be appropriate in the circumstances, including the system's reliability, security and capacity; firms also should have appropriate contingency measures in place • Circular dated 27 November 2014 issued to all licensed corporations and requiring procedures for mitigating cyber security risks: licensed corporations should conduct a self-assessment with a view to (1) preventing, detecting, mitigating and managing (by way of damage control) the risk of potential loss of the firm's own, and investors', information or assets due to cyber security attacks and (2) implement commensurate controls
Swiss Financial Market Supervisory Authority (FINMA)	• Swiss licensees according to the Swiss Collective Investment Schemes Act (CISA) are required to maintain a proper organisational structure, including risk management, internal control system and compliance according to art. 14 (1 c) in connection with art. 12 and 12a of the Swiss Collective Investment Schemes Ordinance (CISO). In principle this also includes proper processes to deal with cyber risks • Additionally, Swiss licensees must comply with the provisions of the Federal Act on Data Protection (FADP) which aims to protect the privacy and fundamental rights of persons when their data is processed *Separately, additional guidance and recommendations have been published by industry associations for the financial sector:* • The Swiss Funds and Asset Management Association (SFAMA) issued its Code of Conduct (CoC), which contains principles with regard to a proper organizational structure (60ff), including an adequate Business Continuity Management (BCM) process (70) • The Swiss Bankers Association (SBA) published its recommendations for Business Continuity Management (BCM) which address, amongst other things, IT systems and IT infrastructure (including communications systems) and IT Disaster Recovery Planning; these detailed recommendations are currently applicable only to Swiss banks and securities dealers