International Association of Risk and Compliance Professionals (IARCP)
1200 G Street NW Suite 800, Washington DC, 20005-6705 USA
Tel: 202-449-9750, Web: www.risk-compliance-association.com

Monday, September 19, 2022

Top 10 risk and compliance related news stories and world events that (for better or for worse) shaped the week's agenda, and what is next

Dear members and friends,

From the moment I read the text of regulation (EU) 2019/2088 on *sustainability related disclosures in the financial services sector (SFDR),* I knew we have a problem. It is not easy to identify and report sustainability risks.

Disclosures to end investors on adverse sustainability impacts, on sustainable investment objectives, or on the promotion of environmental or social characteristics in investment decision-making are *insufficiently developed,* because such disclosures are not yet subject to harmonised requirements. This is changing rapidly.

On 25 September 2015, the UN General Assembly adopted a new global sustainable development framework: the 2030 Agenda for Sustainable Development (the '2030 Agenda'), which has at its core the Sustainable Development Goals (SDGs).

The European Commission Communication of 22 November 2016 on the next steps for a sustainable European future linked the SDGs to the EU policy framework, to ensure that all Union actions and policy initiatives, both within the Union and globally, take the SDGs on board at the outset.

In its conclusions of 20 June 2017, the European Council confirmed the commitment of the European Union and its Member States to the implementation of the 2030 Agenda in a full, coherent, comprehensive, integrated, and effective manner, and in close cooperation with partners and other stakeholders.

From the moment I read the 2015 UN framework, I was expecting the European Regulation and I was considering the consequences for major EU banks, or banks with presence in the EU. The regulation came in 2019, and it had the good old introduction that explains why it is necessary:

"In the absence of harmonised EU rules on sustainability-related disclosures to end investors, it is likely that diverging measures will continue to be adopted at national level and different approaches in different financial services sectors might persist. Such divergent measures and approaches would continue to cause significant distortions of competition because of significant differences in disclosure standards."

So, we need a harmonised approach, let's call it a regulation, that is directly applicable to all EU member states.

The regulation requires financial market participants and financial advisers which provide investment advice *or insurance advice* with regard to insurance-based investment products (IBIPs), regardless of the design of the financial product and the target market, to publish written policies on the integration of sustainability risks and ensure the transparency of such integration.

According to Article 6 (Transparency of the integration of sustainability risks), financial market participants shall include descriptions of the following in pre-contractual disclosures:

(a) the manner in which sustainability risks are integrated into their investment decisions; and
(b) the results of the assessment of the likely impacts of sustainability risks on the returns of the financial products they make available.

Where financial market participants deem sustainability risks not to be relevant, the descriptions referred to in the first subparagraph shall include a clear and concise explanation of the reasons therefor.

What is new - We have an interesting development, the "*Joint report on the extent of voluntary disclosure of principal adverse impact under the Sustainable Finance Disclosure Regulation (SFDR)",* from the three European Supervisory Authorities (ESAs), the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA), and the European Securities and Markets Authority (ESMA).

The ESAs conclude that the *extent of compliance* with voluntary disclosures varies significantly across respondents. The ESAs' assessment is that the *level of compliance* is higher in larger groups.

After my legal studies, I am convinced that the phrases "*extent of compliance"* and *"level of compliance"* simply mean *no compliance*, but this is just my opinion.

Read more at Number 1 below. Welcome to the Top 10 list.

Best regards,

George Lekatis
President of the IARCP
1200 G Street NW Suite 800,
Washington DC 20005, USA
Tel: (202) 449-9750
Email: lekatis@risk-compliance-association.com
Web: www.risk-compliance-association.com
HQ: 1220 N. Market Street Suite 804,
Wilmington DE 19801, USA
Tel: (302) 342-8828

Number 1 (Page 6)

Joint report on the extent of voluntary disclosure of principal adverse impact under the Sustainable Finance Disclosure Regulation (SFDR)

Number 2 (Page 9)

FSB Annual Financial Report

Number 3 (Page 11)

Statement on PCAOB Amendments to Strengthen Auditing Standards for Audits Involving Multiple Firms

SEC Chair Gary Gensler

Number 4 (Page 13)

Planning and Supervision of Audits Involving Other Auditors and Dividing Responsibility for the Audit with Another Accounting Firm

Number 5 (Page 17)

Looking for the 'Sliver' lining: Hunting for emerging command-and-control frameworks

Number 6 (Page 19)

Regulatory Consistency Assessment Programme (RCAP): Assessment of Basel Committee's large exposures framework – European Union

BIS

Number 7 (Page 22)

Regulatory Consistency Assessment Programme (RCAP): Assessment of Basel Committee's Net Stable Funding Ratio standard - European Union

BIS

Number 8 (Page 26)

What Does it Take to Get to Net Zero

Ravi Menon, Managing Director, Monetary Authority of Singapore, at the Economic Society of Singapore Annual Dinner 2022

Number 9 (Page 39)

Ransomware: Publicly Reported Incidents are only the tip of the iceberg

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

Number 10 (Page 45)

The Cyber Defense Review

VOLUME 7, NUMBER 3, SUMMER 2022

THE CYBER DEFENSE REVIEW

Number 1

Joint report on the extent of voluntary disclosure of principal adverse impact under the Sustainable Finance Disclosure Regulation (SFDR)

Regulation (EU) 2019/2088 of the European Parliament and of the Council of 27 November 2019 on sustainability-related disclosures in the financial services sector (hereinafter 'SFDR') tasks the ESAs, under its Article 18, to 'take stock of the extent of voluntary disclosures in accordance with point (a) of Article 4(1) and point (a) of Article 7 (1)' and that 'By 10 September 2022, and every year thereafter, the ESAs shall submit a report to the Commission on best practices and make recommendations towards voluntary reporting standards'.

Article 18 also states: 'That annual report shall consider the implications of due diligence practices on disclosures under this Regulation and shall provide guidance on this matter'.

Contents

To gather information for the purposes of this report, the European Supervisory Authorities (ESAs) have launched through the Joint Committee (JC), as well as through the relevant Standing Committees of the ESAs, a survey of its members, the National Competent Authorities ('NCAs'), with the purpose of gathering feedback on the current state of entity level voluntary disclosures under Article 4 (1) point (a) SFDR.

With the view of getting a complete picture of the state of voluntary disclosures in the market, the ESAs have decided to ask NCAs for their feedback also on the disclosures for financial market participants (FMPs) choosing to explain why they do not consider adverse impacts of investment decisions on sustainability factors as per Article 4 (1) (b) SFDR, even if not explicitly requested by Article 18 SFDR.

The survey has not covered disclosures under Article 7 (1) SFDR as it is expected that FMPs will start applying those by 30 December 2022.

The ESAs have carefully analysed the 33 responses received and developed an indication of good examples of best practices observed by April 2022 and preliminary recommendations.

Those are based on a combination of responses from the NCAs, of which the most relevant extracts are reported anonymously in Section 4.3 of this report, and ESAs' staff's desk-based research.

The first report's preliminary conclusions are that the extent of compliance with voluntary disclosures under Article 4 (1) (a) varies significantly across jurisdictions and FMPs under the scope of SFDR, and it is difficult to identify definite trends.

It was not possible to draw conclusions in terms of the differences across FMPs based on size, nature, and scope of activities.

At this stage, the ESAs have identified that the disclosures for FMPs that do not take into account adverse impact of investment decisions on sustainability factors under Article 4 (1) (b) are lacking in detail, and FMPs largely fail to provide clear reasons for why they do not do so, with insufficient information as to whether and when they intend to consider such adverse impacts.

Finally, NCAs have reported overall low level of disclosure of the degree of alignment with the objective of the Paris agreement, with disclosures on the alignment being vague and high level.

Section 2 this report includes the background and rationale of this exercise and lessons learned from the first year of implementation of the voluntary disclosures, based on responses from NCAs.

Section 3 provides an overview of good examples of best practices, and other less good examples of voluntary disclosures under Article 4 (1) (a) and (b) SFDR.

The last part of this section also includes recommendations to the Commission and NCAs.

The Annex provides an overview of the questions included in the survey with some highlights from the responses received from the NCAs.

The ESAs would like to state that SFDR has become applicable on 10 March 2021. However, as the detailed Regulatory Technical Standards (RTS) on these disclosures are not yet applicable and given the still emerging NCAs' supervisory practices on voluntary disclosures by FMPs, the indications of good examples of best practices and recommendations included in this report must be considered preliminary at this stage and will be complemented further in subsequent reports.

In addition, as it is too early to offer meaningful guidance on the implications for due diligence disclosures more generally, the ESAs plan to address this in future iterations of the report.

Finally, the future iterations will also cover voluntary disclosures under Article 7 (1), which will only be fully applicable from 30 December 2022.

In terms of next steps, the Commission may consider the ESAs' findings and take those into account in any preliminary evaluation on the functioning of the SFDR.

The ESAs may also consider the findings in the work on the new mandate received on 28 April 2022 to review the PAI framework.

To read more:
https://www.eiopa.europa.eu/sites/default/files/publications/reports/jc-2022-35-joint-esas-report-on-the-extent-of-voluntary-disclosures-of-pai-under-sfdr.pdf

Number 2

FSB Annual Financial Report

The Financial Stability Board (FSB) coordinates, at the international level, the work of national financial authorities and international standard - setting bodies in order to develop and promote the implementation of effective regulatory, supervisory and other financial sector policies.

In collaboration with the international financial institutions, the FSB also addresses vulnerabilities affecting financial systems in the interest of global financial stability.

This report contains the financial statements of the FSB, for the 12-month period from 1 April 2021 to 31 March 2022. It also provides details on the FSB governance arrangements and the transparency and accountability mechanisms.

A detailed explanation of the activities undertaken to implement the mandate and tasks of the FSB is provided in the FSB's Annual Report, which describes the FSB's work to promote global financial stability. More information about the FSB's activities is available on its website.

Financial Stability Board in numbers

68 member institutions, comprising ministries of finance, central banks, and supervisory and regulatory authorities from 25 jurisdictions, 10 of which are emerging market and developing economies, as well as 10 international organisations and standard-setting bodies; 6 Regional Consultative Groups reaching out to 70 other jurisdictions around the world; and 35 Secretariat staff.

The FSB was established in April 2009 as the successor to the Financial Stability Forum (FSF).

In January 2013, the FSB established itself as an association ("Verein") under Swiss law with its office at the Bank for International Settlements (BIS), Centralbahnplatz 2, Basel – 4002, Switzerland.

The FSB's membership comprises authorities from jurisdictions that are responsible for maintaining financial stability, such as ministries of finance, central banks, supervisory and regulatory authorities; international financial institutions; and international standard-setting, regulatory, supervisory and central bank bodies.

As part of its mandate, the FSB:

(a) assesses vulnerabilities affecting the global financial system and identifies and reviews on a timely and ongoing basis within a macroprudential perspective, the regulatory, supervisory and related actions needed to address them, and their outcomes;

(b) promotes coordination and information exchange among authorities responsible for financial stability;

(c) monitors and advises on market developments and their implications for regulatory policy;

(d) advises on and monitors best practice in meeting regulatory standards;

(e) undertakes joint strategic reviews of and coordinates the policy development work of the international standard-setting bodies (SSBs) to ensure their work is timely, coordinated, focused on priorities and addressing gaps;

(f) sets guidelines for and supports the establishment of supervisory colleges;

(g) supports contingency planning for cross-border crisis management, particularly with respect to systemically important firms;

(h) collaborates with the IMF to conduct Early Warning Exercises;

(i) promotes member jurisdictions' implementation of agreed commitments, standards and policy recommendations through monitoring of implementation, peer review and disclosure; and

(j) undertakes any other tasks agreed by its Members in the course of its activities and within the framework of its Charter.

To read more: https://www.fsb.org/wp-content/uploads/P170822.pdf

Number 3

Statement on PCAOB Amendments to Strengthen Auditing Standards for Audits Involving Multiple Firms

SEC Chair Gary Gensler

The Commission approved the Public Company Accounting Oversight Board's (PCAOB) updated standards for audits that involve multiple auditing firms.

I was pleased to support the amended standards because they will strengthen the requirements for lead auditors who supervise other auditors in an audit, helping to enhance audit quality and protect investors.

Over the years, the growing complexity and international operations of public companies has led auditors increasingly to rely on other auditors — working across different firms, countries, and even languages — in completing an audit.

Last year, for example, 26 percent of all issuer audit engagements used multiple auditors, and more than half of large accelerated filer audits used multiple auditors.

Given the challenges that such multi-firm audits present, it is important that there be robust standards for how lead auditors supervise, communicate with, and coordinate with other auditors on the audit engagement.

The PCAOB's updated standards make enhancements across two broad areas.

First, the amended standards specify certain procedures for lead auditors to perform when supervising other auditors.

Second, they require lead auditors to prioritize their supervisory activities around higher-risk areas in the audit.

I thank the PCAOB for their work to update this auditing standard, the first adopted since the Board was newly constituted. I look forward to the

additional standard-setting work the PCAOB will undertake to live up to its founding vision under the Sarbanes-Oxley Act.

If Sarbanes-Oxley, signed into law 20 years ago, meets its full potential, trust in our markets can grow — and that benefits investors and issuers alike.

To read more:
https://www.sec.gov/news/statement/gensler-statement-pcaob-amendments-081222?fbclid=IwAR05zcpyfn2UhHK61nOoP6zsVr-zVReiWquSLUV4jr9iu6bfahwkQfSypSg

Number 4

Planning and Supervision of Audits Involving Other Auditors and Dividing Responsibility for the Audit with Another Accounting Firm

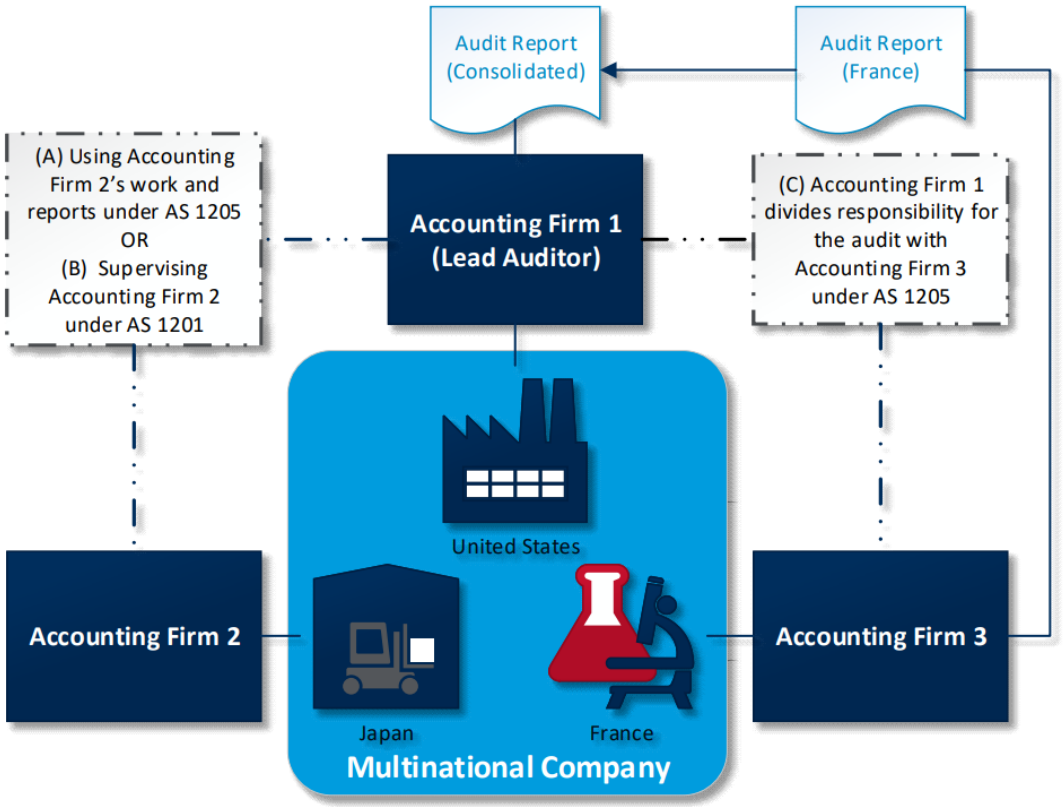
PCAOB
PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD

The Public Company Accounting Oversight Board ("PCAOB" or the "Board") is adopting amendments to its auditing standards to strengthen the requirements and responsibilities that apply to auditors who plan and perform audits that involve other accounting firms and individual accountants.

The amendments are designed to improve the quality of audits in these circumstances by increasing the lead auditor's involvement in and evaluation of the work of other auditors, and to align the applicable requirements with the PCAOB's risk-based supervisory standards.

Table of Contents

Figure 1. Example of an Audit Involving Other Accounting Firms



EXECUTIVE SUMMARY

We are amending our auditing standards to strengthen requirements for planning and supervising audits involving accounting firms and individual accountants (collectively, "other auditors") outside the accounting firm that issues the auditor's report (the "lead auditor").

In these audits, the lead auditor issues the audit report on the company's consolidated financial statements, but other auditors often perform important work on the audit.

The roles of other auditors have increased as companies' global operations have grown. In addition, we are adopting a new auditing standard that will apply when the lead auditor divides responsibility for an audit with another accounting firm ("referred-to auditor").

Working with other auditors and referred-to auditors can differ from working with people in the same firm, creating challenges in coordination and communication.

These challenges can lead to misunderstandings about the nature, timing, and extent of their work and can reduce audit quality.

It is important for investor protection that the lead auditor adequately plan and supervise the work of other auditors so that the audit is performed in accordance with PCAOB standards and provides sufficient appropriate evidence to support the lead auditor's opinion in the audit report.

This rulemaking is intended to increase and improve the lead auditor's involvement in and evaluation of the other auditors' work. We believe that the heightened attention to other auditors' work will improve communication among auditors and the lead auditor's ability to prevent or detect deficiencies in that work, and thus enhance the quality of audits involving other auditors and promote investor protection.

The amendments to the Board's auditing standards are intended to improve PCAOB standards principally by

(i) applying a risk-based supervisory approach to the lead auditor's oversight of other auditors and

(ii) requiring that the lead auditor perform certain procedures when planning and supervising an audit that involves other auditors. The amendments take into account recent practice developments in the lead auditor's oversight of other auditors' work, including the greater use of communication technology. In brief, the amendments:

- Require that the engagement partner determine whether his or her firm's participation in the audit is sufficient for the firm to carry out the responsibilities of a lead auditor and report as such. The amendments also provide considerations for the engagement partner to use in making this determination and require that the audit's engagement quality reviewer review the determination.

- Require that the lead auditor, when determining the engagement's compliance with independence and ethics requirements, understand the other auditors' knowledge of those requirements and experience in applying them. The amendments also require that the lead auditor obtain and review written affirmations regarding the other auditors' policies and procedures related to those requirements and regarding compliance with the requirements, and a description of certain auditor-client relationships related to independence. In addition, the amendments require the sharing of information about changes in circumstances and the updating of affirmations and descriptions in light of those changes.

- Require that the lead auditor understand the knowledge, skill, and ability of other auditors' engagement team members who assist the lead

auditor with planning and supervision, and obtain a written affirmation from other auditors that their engagement team members possess the knowledge, skill, and ability to perform assigned tasks.

- Require that the lead auditor supervise other auditors under the Board's standard on audit supervision and inform other auditors about the scope of their work, identified risks of material misstatement, and certain other key matters. The amendments also require that the lead auditor and other auditors communicate about the audit procedures to be performed, and any changes needed to the procedures. In addition, the amendments require the lead auditor to obtain and review written affirmations from other auditors about their performance of work in accordance with the lead auditor's instructions, and to direct other auditors to provide certain documentation about their work.

- Provide that, in multi-tiered audits, a first other auditor may assist the lead auditor in performing certain required procedures with respect to second other auditors.

To read more:
https://pcaob-assets.azureedge.net/pcaob-dev/docs/default-source/rulemaking/docket042/pcaob-other-auditors-adopting-release-6-21-2022.pdf?sfvrsn=c3712668_2

Number 5

Looking for the 'Sliver' lining: Hunting for emerging command-and-control frameworks

Microsoft

Microsoft has observed the Sliver command-and-control (C2) framework now being adopted and integrated in intrusion campaigns by nation-state threat actors, cybercrime groups directly supporting ransomware and extortion, and other threat actors to evade detection.

We've seen these actors use Sliver with—or as a replacement for—Cobalt Strike. Given Cobalt Strike's popularity as an attack tool, defenses against it have also improved over time. Sliver thus presents an attractive alternative for actors looking for a lesser-known toolset with a low barrier for entry.

First made public in late 2019 and advertised to security professionals, Sliver is an open-source framework that's available on GitHub and includes many common C2 framework features such as support for multiple simultaneous operators, multiple listener types, user-developed extensions, and payload generation. Since December 2020, we've observed threat actors adopting Sliver into their arsenal.

Among its adopters is the prolific ransomware-as-service (RaaS) affiliate DEV-0237. More recently, we've seen cybercrime actors historically tied to human-operated ransomware now deliver Sliver and various post-compromise tools using Bumblebee malware (also known as COLDTRAIN) as an initial access loader. Customers can learn more about Bumblebee in our Threat Analytics report available in the Microsoft 365 Defender portal.

In this blog, we share how the researchers behind Microsoft Defender Experts for Hunting analyzed Sliver and used both lab-simulated attacks and real-world threat activity to create hunting queries to surface Sliver and other C2 frameworks.

Threat hunting: Part art(ifact), all science

For security researchers, there's a distinction between hunting and detection. For novel threats, researchers try to strike a balance between high-fidelity detection rules identifying a specific, known malware family, threat actor, or class of behavior and low-fidelity hunting rules, which generate more false positives but also more generically capture a technique and its derivatives.

The following sections illustrate the art and science of how these lower-fidelity rules help threat hunters measure and contextualize suspicious observations to find novel or stealthy threats.

Sleuthing Sliver

Threat actors use C2 frameworks to manage their access to compromised hosts and networks during an intrusion. A C2 framework usually includes a server that accepts connections from implants on a compromised system, and a client application that allows the C2 operators to interact with the implants and launch malicious commands.

Many threat actors integrate public, open-source C2 framework options into their arsenal because these have a low barrier to entry and offer several advantages for attackers like low cost, ease of modification, and difficult attribution. As previously mentioned, Sliver is one such open-source framework. Although Sliver is somewhat new, the TTPs it implements are common across many frameworks.

Below are examples of how Defender Experts hunt for these TTPs to identify Sliver and other emerging C2 frameworks in customer environments.

Infrastructure

Sliver, like many C2 frameworks, supports various network protocols such as DNS, HTTP/TLS, MTLS, and TCP. It can also accept implant or operator connections and host files to impersonate a benign web server.

The first step in testing any C2 framework is starting listeners and scanning them to identify anomalies. Some common artifacts are unique HTTP header combinations and JARM hashes, the latter of which are active fingerprinting techniques for TLS servers. RiskIQ has shared such a methodology for Sliver and Bumblebee detection.

To read more:
https://www.microsoft.com/security/blog/2022/08/24/looking-for-the-sliver-lining-hunting-for-emerging-command-and-control-frameworks/

Number 6

Regulatory Consistency Assessment Programme (RCAP): Assessment of Basel Committee's large exposures framework – European Union

Through its Regulatory Consistency Assessment Programme (RCAP), the Basel Committee monitors the timely adoption of regulations by its members, assesses the regulations' consistency with the Basel framework and examines the consistency of banks' calculation of the prudential ratios across jurisdictions. The RCAP also helps member jurisdictions to identify and assess the materiality of any deviations from the Basel framework.

This report describes the Committee's assessment of the implementation of the Basel Committee's large exposures framework (LEX) in the European Union (EU). The EU's LEX regulations have been assessed as **largely compliant.**

In the EU, the LEX requirements were first introduced through Regulation (EU) No 575/2013, and then amended for improved alignment with the Basel LEX framework through Regulation (EU) 2019/876, supplemented by a series of acts adopted by the EC and Guidelines issued by the EBA.

The amendment to LEX requirements was published on 7 June 2019 and became applicable from 28 June 2021.

Overall, as of end-March 2022, the LEX regulations in the EU are assessed as largely compliant with the Basel LEX standards.

This is one notch below the highest overall grade. The three components of the Basel LEX standard (scope and definitions; minimum requirements and transitional arrangements; and value of exposures) are assessed as compliant, largely compliant, and compliant, respectively.

The overall grade is driven by a potentially material finding related to the limit applicable to trading book exposures and nine findings that were deemed not material.

For trading book exposures, the EU regulations allow for the LEX limit to be exceeded up to 600% of a bank's Tier 1 capital.

In addition, this report identified an item for follow-up assessment (see Annex 4). It was noted that the EC has proposed an amendment to the

current provisions on the possibility of using own volatility estimates via the deletion of the corresponding provisions in the CRR, which should be subject to review in a future RCAP assessment.

The Assessment Team noted that the LEX regulations in the EU are super-equivalent to the Basel LEX framework in one area.

In accordance with the methodology and guidance provided in the RCAP Handbook for jurisdictional assessments, the stricter rules have not been taken into account as mitigants for the overall or component-level assessment of compliance.

Regulatory system

The EU prudential framework for credit institutions is laid down in two pieces of (Level 1) legislation, namely a Regulation and a Directive, as enacted by the European Parliament and the Council and legally enforceable in all EU Member States.

The Capital Requirements Regulation (CRR, Regulation (EU) No 575/2013) establishes a "single rule book" containing Pillar 1 and Pillar 3 requirements for the EU's entire banking system and is directly applicable and binding in its entirety. This means that it applies directly, without having to be transposed into national law.

The fourth Capital Requirements Directive (CRD IV) is legally binding and must be transposed into national law. It contains rules on authorisation, governance, risk management and buffer requirements.

It also requires Member States to vest competent authorities with sufficient (Pillar 2) powers to address particular risks that are not well covered by the requirements contained in the CRR and to impose sanctions.

The CRR and the CRD IV are complemented or implemented by (Level 2) Binding Technical Standards (BTS) that are drafted by the EBA, based on mandates provided in the CRR and the CRD IV, and adopted by the EC.

BTS are divided into Regulatory Technical Standards (RTS) and Implementing Technical Standards (ITS).

RTS, which are adopted by means of delegated acts, supplement or amend certain nonessential elements of an EU legislative text (Regulation or Directive). ITS, which are adopted by means of implementing acts, aim at ensuring consistent implementation of legislative acts. BTS are legally binding and directly applicable in all Member States.

The EBA also issues (Level 3) Guidelines and Recommendations that elaborate on how requirements set by the EU law are to be applied by European regulators and supervisors.

Although these Guidelines and Recommendations are not legally binding, supervisory authorities across the EU must make every effort to comply with them by incorporating them into supervisory practices as appropriate. Supervisory authorities are obliged to inform the EBA of their compliance or intention to comply with them and to also explain the reasons for any non-compliance ("comply or explain").

All non-compliance instances and the related reasons are placed in the public record. The RCAP EU assessment relied upon the legal force of Directives, Regulations and BTS. It also took into account the Guidelines and Recommendations of the EBA to the extent that confirmations were received from the Member States that they comply with these Guidelines and Recommendations.

To read more: https://www.bis.org/bcbs/publ/d536.pdf

Assessment grades — Table 1

Component of the Basel large exposures framework	Grade
Overall grade	LC
Scope and definitions	C
Minimum requirements and transitional arrangements	LC
Value of exposures	C

Assessment scale: C (compliant), LC (largely compliant), MNC (materially non-compliant) and NC (non-compliant).

Number 7

Regulatory Consistency Assessment Programme (RCAP): Assessment of Basel Committee's Net Stable Funding Ratio standard - European Union

BIS

Through its Regulatory Consistency Assessment Programme (RCAP), the Basel Committee monitors the timely adoption of regulations by its members, assesses the regulations' consistency with the Basel framework and examines the consistency of banks' calculation of the prudential ratios across jurisdictions. The RCAP also helps member jurisdictions to identify and assess the materiality of any deviations from the Basel framework.

This report describes the Committee's assessment of the implementation of the Basel Committee's Net Stable Funding Ratio (NSFR) standard in the European Union (EU). The EU's NSFR regulations have been assessed as **largely compliant.**

The EU NSFR framework was issued in June 2019 by means of Regulation (EU) 2019/876 of the European Parliament and of the Council of 20 May 2019.

The NSFR disclosure and supervisory reporting requirements were laid down through Commission Implementing Regulation (EU) 2021/637 of 15 March 2021 and Commission Implementing Regulation (EU) 2021/451 of 17 December 2020.

The abovementioned NSFR regulations came into force on 28 June 2021 and apply to all credit institutions and systemic investment firms in the EU.

Overall, as of end-March 2022, the NSFR regulations in the EU are assessed as largely compliant with the Basel NSFR standard.

This is one notch below the highest overall grade.

Three of the four components of the Basel NSFR standard (scope, minimum requirements, and application issues; available stable funding (ASF); and disclosure requirements) are assessed as compliant.

The remaining component, required stable funding (RSF), is assessed as largely compliant. This component grade is driven by the cumulative impact of nine not material findings.

In addition, this report identified an item for follow-up assessment. It was noted that the RSF factors for certain types of transaction would be adjusted in aligning the EU regulations with the Basel NSFR standard by June 2025, which should be subject to review in a future RCAP assessment.

Taking effect on 1 January 2014, the CRR and the CRD IV are the main regulatory texts on prudential banking regulation in the EU.

By means of an amendment to the CRR, Regulation (EU) 2019/876 (CRR II) continued the EU's implementation of the Basel standards including the NSFR.

The amendments were adopted on 20 May 2019 and published on 7 June 2019. The NSFR requirements became applicable as of 28 June 2021, while the RSF factors for certain types of transaction will be phased in by June 2025.

The CRD IV contains general provisions on liquidity risk management and supervision. Certain provisions related to supervision of liquidity were amended by Directive (EU) 2019/878, which was adopted on 20 May 2019 and published on 7 June 2019.

Member States had until 28 December 2020 to implement the amendments in national law.

Further, the CRR II provided a mandate for the EBA to develop ITS to specify uniform templates for disclosure and for supervisory reporting with regard to the NSFR.

As such, Commission Implementing Regulation (EU) 2021/637 of 15 March 2021 and Commission Implementing Regulation (EU) 2021/451 of 17 December 2020 were published, which outlined the detailed disclosure and supervisory reporting requirements, respectively.

The standards became applicable on 28 June 2021 and the first reporting reference date was 30 June 2021.

In the EU, the NSFR framework applies to all credit institutions,7 on both an individual and consolidated basis, unless competent authorities do not apply supervision on an individual basis where they deem this appropriate.

Authorities may permit small and non-complex institutions to use a simplified methodology for the calculation and supervisory reporting of the NSFR.

The Assessment Team considered the NSFR requirements applicable to a sample of EU internationally active banks as of end-March 2022.

The assessment had two dimensions:

- a comparison of EU regulations with the Basel NSFR standard to ascertain that all the required provisions have been adopted (completeness of the regulations); and

- whether there are any differences in substance between the EU regulations and the Basel NSFR standard and, if so, their significance (consistency of the regulations).

In its assessment, the Assessment Team considered all binding documents that effectively implement the Basel NSFR standard in the EU. Annex 2 lists the Basel standards used as the basis for the assessment.

The assessment did not evaluate the adequacy of liquidity or the resilience of the banking system in the EU or the supervisory effectiveness of EU authorities.

The Assessment Team evaluated the materiality and potential materiality of identified deviations between the Basel NSFR standard and the EU regulations.

The evaluation was made using a sample of 13 EU internationally active banks.

Together, these banks comprise about 61% of the assets of internationally active banks in the EU. In addition, the Assessment Team reviewed the non-quantifiable impact of identified deviations and applied expert judgment as to whether the EU regulations meet the Basel NSFR standard in letter and in spirit.

The materiality assessment is summarised in Annex 4, which also lists the sample of banks. The outcome of the assessment is summarised using a four-grade scale, both at the level of each of the four key components of the Basel NSFR framework and of the overall assessment of compliance.

The four grades are compliant (C), largely compliant (LC), materially non-compliant (MNC) and noncompliant (NC).

To read more: https://www.bis.org/bcbs/publ/d535.pdf

Assessment grades — Table 1

Component of the Basel NSFR framework	Grade
Overall grade	LC
Scope, minimum requirement and application issues	C
Available stable funding (numerator)	C
Required stable funding (denominator)	LC
NSFR disclosure requirements	C

Assessment scale: C (compliant), LC (largely compliant), MNC (materially non-compliant) and NC (non-compliant).

Number 8

What Does it Take to Get to Net Zero

Ravi Menon, Managing Director, Monetary Authority of Singapore, at the Economic Society of Singapore Annual Dinner 2022

ESM Goh, Dr Euston Quah, distinguished guests, ladies and gentlemen. It is both an honour and pleasure to speak to you.

There are many pressing issues I could talk about today. The world is just emerging from the most devastating pandemic in over a century, with far-reaching changes whose effects will be felt for years to come.

A major war has broken out between the two largest countries in Europe, heightening geopolitical risks and setting off a food and energy crisis across the world. The global economy is facing the sharpest surge in inflation and fastest pace of monetary policy tightening in 40 years, with highly uncertain consequences.

Instead, I want to talk about what I think is the mother of all challenges facing the world today, and for the next few decades – climate change. Long after our conjunctural challenges of war, disease, and inflation are behind us, the climate crisis will still be with us, only more intense, more urgent, more disruptive.

CLIMATE CHANGE

Climate change is already happening. Over the last three decades, the number of registered severe weather events has tripled. Over the last two decades, the rate of increase in sea levels has doubled. Over the last decade, the pace of ice loss in the Arctic and Antarctic has tripled.

This year, wildfires and heatwaves of unprecedented ferocity have swept across Europe, North America, and Australia, while record rainfall in countries ranging from India to America have caused devastating floods. Climate change is happening at a faster pace than predicted by early climate models.

It is critical that we stop putting more carbon into the atmosphere by 2050. According to climate scientists, to avoid catastrophic and irreversible climate change, global warming needs to be kept within 1.5 degrees Celsius above pre-industrial levels. This in turn requires that global greenhouse

gas emissions must reach net zero around 2050, meaning we remove whatever greenhouse gases we put into the atmosphere every year. This is what more than 190 countries resolved as part of the Paris Agreement in 2015.

The world is currently far from a net-zero emissions trajectory. To limit global warming to 1.5 degrees Celsius, global greenhouse gas emissions must peak by 2025 and come down about 45% by 2030 relative to 2019 levels. We are currently not on track to achieve this. Even if all countries follow through on commitments made in the Paris accords, carbon emissions will come down by just 7.5% by 2030.

This means 1.5 degrees Celsius is almost out of reach. According to the latest report by the United Nations Intergovernmental Panel on Climate Change (IPCC), global warming has already reached 1.1 degrees Celsius above pre-industrial levels, the warmest in 125,000 years.

Based on current policies, global temperatures are expected to rise by 2.7 degrees Celsius above pre-industrial levels by 2100. Even according to the most optimistic estimates of emission cut pledges made at COP-26, the world is on course to heat up by 1.8 degrees Celsius. According to the IPCC, to fall back below the 1.5 degrees Celsius target, it would be necessary to remove from the atmosphere a decade or two of carbon emissions.

If the current emissions trajectory continues, the world will likely experience climate catastrophe. In his book, Hothouse Earth, Bill McGuire, emeritus professor of geophysical and climate hazards at University College London, argues that there is now no chance of the world avoiding a pervasive climate breakdown.

When temperatures rise beyond 1.5 degrees Celsius within the next 10 years, we can expect a world plagued by intense summer heat, extreme drought, devastating floods, reduced crop yields and food supplies, higher incidence of vector-borne diseases, rapidly melting ice sheets, and surging sea levels. Many parts of the world will become less hospitable for human habitation. By some estimates, climate change may force more than one billion people to migrate by 2050.

THE CHALLENGE OF DECARBONISATION

2020 to 2030 is the critical decade for climate action. Net zero commitments for 2050 are fine and good but a credible trajectory towards that goal will be substantially determined by 2030. While a growing number of countries and companies have set net-zero targets, very few have credible plans to meet them.

The problem is that countries and companies alike are pledging to hit targets in almost three decades' time without committing to action for which they can be held accountable in the short term. To achieve net-zero by 2050, the necessary policies and the associated investments must be made between now and 2030.

Singapore is firmly committed to doing its part in the global effort to reduce greenhouse gas emissions. Last year, the government launched the Singapore Green Plan, which sets out a road map towards sustainable development, a green economy, and net zero emissions. Singapore aims to peak carbon emissions around 2030 and to achieve net zero by or around mid-century. If anything, the direction of travel in the coming years can only be towards greater climate ambition, not less.

The world should be upfront about the cost of decarbonisation and have concrete plans to support those adversely affected. There will no doubt be opportunities in green technologies and industries, and the long-term cost of doing nothing will be much more than the cost of mitigation measures. But decarbonisation will impose substantial short-term economic costs and have profound distributional implications.

Like all economic transformations, the green transition will involve winners and losers, and unless this is recognised and dealt with, the sustainability agenda will lose social legitimacy. If we do not support the losers, there will be a strong backlash against the shift to a greener, cleaner future, much like the backlash we have seen against globalisation by those who were adversely affected by it.

The transition to net zero will likely entail the biggest economic and societal transformation since the Industrial Revolution. As the environmental scientist Vaclav Smil, in his book How the World Really Works, declares rather ominously, "We are a fossil-fuelled civilization whose technical and scientific advances, quality of life, and prosperity rest on the combustion of huge quantities of fossil carbon." To transit from such a fossil fuel civilisation to a net zero world will require considerable economic restructuring, significant technological breakthroughs, and substantial financial investments.

Getting to net zero will not be easy and will require five transformative changes:

- a price on carbon;
- a shift to cleaner energy;
- a greening of the economy;
- a pivot to transition finance;

- a sustainable lifestyle.

CARBON PRICING

A meaningful price for carbon is the single most important measure to help decarbonise the economy. A carbon price can be achieved in three ways: a tax on carbon emissions; or a system for trading emissions permits; or regulatory limits on emissions that could be translated into an implicit carbon price.

Without getting the price of carbon right, most sustainability efforts will not make economic sense and not gain traction. The right price on carbon sends a powerful signal across the entire economy: it induces consumers to reduce demand for carbon-intensive goods and services; firms to move to low carbon technologies; innovators to invent and develop new low carbon products and processes; and investors to fund and commercialise them. The invisible hand of the carbon price incentivises and coordinates emissions-reduction efforts in ways that regulation cannot achieve.

While carbon pricing has gained traction globally, it needs to be higher and applied more broadly. The right price of carbon is the social cost it imposes on the environment. According to the World Bank, less than 5% of the emissions covered by a carbon pricing initiative are priced at a level consistent with achieving the goals of the Paris Agreement, namely US$40-80 per tonne of carbon dioxide by 2020 and US$50-90 per tonne by 2030.

The idea of a federal carbon tax remains political anathema in the United States. Even the European Emissions Trading System currently covers only about 50% of the EU's greenhouse gas emissions and gives many allowances for free.

Singapore will progressively raise its carbon taxes from 2024. The current level of S$5 per tonne of CO2 equivalent will be raised to S$25 per tonne in 2024 and 2025, and S$45 in 2026 and 2027, with a view to reaching S$50-80 by 2030. This translates to a carbon price of roughly US$36-58 per tonne of CO2 equivalent in 2030.

It is somewhat below the US$50-90 estimated by the World Bank of what a net-zero consistent price of carbon should be in 2030 but Singapore's carbon tax covers about 80% of our national greenhouse gas emissions, much broader than in most countries. Singapore is also progressive in having a long tradition of high petrol taxes and no subsidies for fuel or electricity. Together, these policies will help to sharpen the substitution

effects necessary for shifting to cleaner transportation modes and improving energy efficiency as carbon taxes rise.

Let me make three observations about carbon pricing.

First, carbon taxes should be implemented equitably so that they do not overly burden low-income households and SMEs. Singapore does not intend to derive extra net revenue collected from the carbon tax. The carbon tax revenue will be used to cushion the impact on lower-income households through U-Save rebates and incentives to switch to energy efficient appliances.

Carbon tax revenues will also be directed to SMEs to help boost their energy efficiency and decarbonisation efforts. This is an economically sound approach: it retains the desired allocative effects of higher carbon taxes while dampening its distributional consequences.

Second, green subsidies are useful complements to carbon pricing but they are not substitutes. Subsidies for clean technology and energy efficiency can help to speed up the transition towards sustainability. But they often make economic sense only if combined with some form of carbon pricing.

Take for instance subsidies for electric vehicle purchases and infrastructure. Without a price on carbon that is in turn reflected in electricity prices, subsidies for electric vehicles will likely lead to more such cars on the road with little reduction in the number of petrol-powered cars or shift towards cleaner sources of electricity generation. Indeed, it has been observed in California that electric vehicles are bought mostly by households with multiple cars, as a supplement to petrol-powered cars.

Third, a global minimum carbon price makes economic sense but needs to be carefully designed. As emphasised by economist William Nordhaus, there should be a common, harmonised price of carbon, across sectors and across countries, that is equal to the global social cost of carbon. Every molecule of carbon dioxide that is emitted imposes the same social cost, regardless of where it is emitted from. It is unlikely that there will be an international agreement on a single global carbon price. But there are two ways in which global convergence in carbon pricing can come about.

The first is through carbon credits and markets. If a sufficient number of countries have carbon taxes, it would facilitate cross-border trading of carbon credits which will help to drive carbon prices closer.
The second is through the carbon border adjustment mechanism, or CBAM, which is a tariff that prices the carbon content of imported goods the same as the carbon emitted in domestic production.

Advocates of the CBAM see it as a way to ensure that internalising a global externality in some economies does not lead to expansion of more polluting firms elsewhere. But opponents view CBAMs as being potentially protectionist and disproportionately hurting developing countries who lack the capabilities and support to decarbonise.

Singapore will do well to prepare for a future where CBAMs cover a significant part of world trade. CBAMs are likely to be a reality, especially if several major economies agree on a global minimum carbon price. The EU has already proposed a CBAM. A well-designed CBAM that does not raise barriers to trade, is compliant with WTO rules, and gives some relief to the poorest countries who are also small emitters, is not a bad outcome.

CLEANER ENERGY

The second imperative for the net zero transition is a decisive shift towards cleaner energy. According to the IPCC, to have a good chance of limiting global warming to 1.5 degrees Celsius, global consumption of coal, oil, and gas must start declining immediately and steeply. This is unlikely to happen.

The growth in renewable energy has been spectacular but not sufficient to meet growing energy demand. Despite a 50-fold increase in the supply of new renewable energy in the last two decades, fossil fuels continue to account for more than 80% of global primary energy consumption.

One of the reasons is that about 750 million people in the world still lack access to electricity. For them, the priority is having the lights on at an affordable price, not how much carbon dioxide is emitted in its production. Most of the people living in sub-Saharan Africa in 2020 consume no more energy per capita than the people of France and Germany did in 1860. Providing these poor people a dignified standard of living would require doubling their rate of energy consumption.

According to the International Energy Agency (IEA), the energy transition to achieve net-zero is doable but difficult.

First, even when the world achieves net-zero emissions, fossil fuels will be with us. Energy demand in Asia is expected to double by 2030 on the back of strong economic growth, rising affluence, and urbanisation. Even if overall global energy use falls in the net zero scenario, it will increase in many of the poorest countries. Fossil fuels will continue to play an important role in meeting the energy demands of Asia and Africa. Coal is unlikely to have a role in a net zero world but oil and gas will. The IEA has

projected that if the world reached net zero by 2050, it would still be using nearly half as much natural gas as today and about one-quarter as much oil.

Second, solar and wind power will need to be the largest energy source. The cost of solar and wind energy has fallen dramatically over the past decade and the amount of power generated through these renewables is rapidly catching up to that generated by coal. The IEA has projected photovoltaic capacity jumping twenty-fold between now and mid-century. This is no mean task – it implies by 2030 installing every day the generation capacity of what is currently the world's biggest solar farm.

Third, hydrogen will be an important new hope for decarbonisation. This involves using renewable energy to split water molecules to produce both hydrogen and oxygen. The hydrogen can be burnt as a fuel emitting only water vapour or be put into a fuel cell to make electricity on demand. It can also be used as a feedstock to make more energy-dense compounds such as ammonia, which can serve as a fuel itself.

Hydrogen and ammonia can be critical to the transition to a net-zero world given their potential role in decarbonising hard-to-electrify sectors, such as steel production; fuelling trucks, ships, and other heavy vehicles. All of this is technologically possible but making it economically efficient will require further innovation.

In Singapore, our aim is to progressively decarbonise the power sector. We do not have the land for large solar or wind farms or fast flowing rivers for hydro-electric power. But it helps that Singapore is already less carbon-intensive in power generation than many other countries that still use coal.

We are working to increase the carbon efficiency of natural gas which today accounts for 95% of electricity generation and is likely to remain the dominant energy source for some time.

We are accelerating solar deployment across the island and building viable energy storage systems. Using our reservoirs, we are opening one of the world's largest floating solar energy systems.

We are using transmission lines linked to neighbouring countries to import the renewable energy they produce. Singapore has already started importing from Laos energy from hydroelectric power.
We are exploring geothermal and biomethane technologies as well as small modular reactors using nuclear fission.

GREEN ECONOMY

The third imperative for the net zero transition is to green the economy.

Greening the existing economy is more important than growing new green sectors. Investing in green technologies and renewable energy is important. But such pure green activities are estimated to make up less than 8% of the global economy. Non-green activities – in manufacturing, building and construction, aviation, maritime, agriculture and fisheries - make up the bulk of any economy. To move the needle on emissions reduction, we need transition strategies that progressively reduce the carbon footprint across all sectors.

Let me highlight six challenges associated with greening the global economy.

First, a green economy will rely much more on electricity. The cheapest and easiest way to decarbonise several sectors of the economy, such as cars that run on petrol or heat generated by burning natural gas, is to electrify them and ensure that the electricity is generated from zero or low carbon sources.

According to the Princeton researchers, total electricity usage in the United States will likely be two to four times as great in a fully decarbonised economy compared with today. In the IEA's net zero world, electric vehicle sales would vault from 5% of the car market today to 60% in 2030. This would require building the equivalent of 20 of Tesla's massive "gigafactories" every year this decade.

Second, a green economy will need to be much more energy efficient. Energy intensity — the energy needed to produce a dollar of GDP — will have to improve substantially. The IEA has estimated that, to reach net zero, the rate of improvement in energy intensity would have to go up to more than 4% a year, which is more than double the average rate of the previous decade. Current plans and commitments made by countries will yield an improvement of only 2.8% a year.

Third, a green economy will need to find ways to decarbonise so-called 'hard-to-abate' sectors and activities. There are currently not very good transition pathways for aviation and maritime. There are also some critical materials whose production is hard to decarbonise.

Some 17% of the world's primary energy supply is used just to make four materials – steel, cement, plastic, and ammonia (which is used in fertilisers). These four materials have been described as "pillars of modern civilization". Not only are there no readily available substitutes for these

materials, but also no practical low-carbon ways to produce enough to meet current demand. And the world must actually expand their production as Africa and Asia modernise.

Fourth, the sectoral composition of economies will change. The sectors with the highest greenhouse gas emissions – such as coal, oil and gas power and petroleum products – will be most impacted. They account for about 20% of global GDP. McKinsey estimates that US$2.1 trillion worth of assets in the power sector could be retired or underutilised between now and 2050.

Activities supporting lower-emissions products are likely to grow in importance, ranging from mining lithium for batteries to manufacturing solar panels and charging stations for electric vehicles. Demand will also grow for green services, such as forest management, sustainable engineering and design, green finance, and emissions measurement and tracking solutions.

Fifth, inflation is likely to be higher during the long transition to net zero. Higher energy prices will feed through into the production of many goods, and prices overall will rise. The Bank of England estimates inflation will increase by nearly 0.6 percentage by the early 2020s if there is an orderly transition to net zero and 2 percentage points by the early 2030s if the transition is disorderly.

We are probably seeing a preview of that scenario currently. But it's not just energy prices. Demand will surge for minerals such as copper, aluminium, cobalt, lithium, nickel, and rare earths, which are critical to various clean energy technologies, including wind turbines and electric vehicles.

For example, solar or wind power plants use up to six times more copper than conventional power generation. According to the IEA, a world on track for net-zero in 2050 will need six times as much of these materials in 2040 as it does today. The result is greenflation, or rising prices for these metals and minerals that are essential to renewable energy and technologies.

Sixth, the labour market will undergo a major adjustment. Jobs will be lost in traditional carbon-intensive sectors but new jobs will be created in carbon-neutral industries. It is estimated that about 200 million jobs would be created and 185 million lost globally by 2050 from a net-zero transition. There will be a period of net job losses during the transition: foundry workers will not instantaneously be transformed into building-insulation experts. Worker reskilling and redeployment will thus be crucial.

Identifying skills adjacencies will be a key part of worker retraining programmes.

In Singapore, a comprehensive strategy to green the economy is taking shape, with a focus on boosting energy and resource efficiency and creating good jobs.

In the petrochemical industry, all the major players have committed to reach net zero by 2050 and government agencies, industry players, and research institutes are developing capabilities in carbon capture and storage technologies.

In the maritime industry, investments are being made to help our port terminals become net zero by 2050 and support the provision of low and zero carbon marine fuels such as ammonia, hydrogen, and biofuels.
In road transport, Singapore aims to do away with the internal combustion engine and switch to electric vehicles by 2040.

Singapore enjoys a trust premium; many emerging green services, like the trading of carbon credits and monitoring, reporting, and verifying carbon emissions, are built on trust.

TRANSITION FINANCE

The fourth enabler for the path to net zero is transition finance. A McKinsey report estimates that getting to net zero in 2050 would require about US$9.2 trillion of investment per year. That is US$3.5 trillion per year more than is currently being invested today. As incomes grow and transition policies are legislated, expected spending will increase and narrow the gap. But there will still be a gap in annual spending of about US$1 trillion.

Two areas in finance need urgent action.

First, green finance needs to be complemented by transition finance. The global financial industry has made good progress in harnessing green finance, namely finance to support green projects such as renewable energy or clean technologies. Last year, green and sustainable bond issuance reached US$800 billion, a ten-fold increase from 2015. Where the industry needs to do better is in transition finance – to provide the funding support for companies that are not so green, to become greener. This includes financing, for instance, early retirement of coal-powered plants and decarbonising hard-to-abate activities.

Second, we need to synergise public and private capital through blended finance for green and transition projects. Many sustainability projects in emerging markets pose financial and political risks that are not commensurate with their expected returns. Catalytic or concessionary capital from multilateral development banks, national authorities, and philanthropic organisations can help to share the risk and improve project bankability, thereby attracting private sector capital. There is also scope to recycle capital by taking loans off the balance sheets of commercial banks and multilateral development banks and structuring them in a form that could be subscribed by institutional investors, insurance companies, and sovereign wealth funds. Several blended finance models have been piloted. But they need to be substantially scaled up to channel the extra US$1 trillion in financing needed for the net zero transition.

Singapore is building a comprehensive ecosystem for green and transition finance to facilitate Asia's net zero journey.

We are building capabilities in environmental risk management in the financial sector through climate stress tests.

We are providing grants to defray the costs of issuing green and sustainability-linked loans and bonds.

We are supporting industry efforts to build the infrastructure for a liquid and transparent voluntary carbon credit market in Asia.
We are deploying technology to address data challenges, such as through an ESG registry to maintain provenance of green certifications and an ESG disclosure platform to allow listed companies to upload corporate sustainability data in a structured and efficient manner.

SUSTAINABLE LIFESTYLE

The fifth and last key to achieving net zero: a sustainable lifestyle. While many of the changes necessary to mitigate climate change are in the realm of public policies, business practices, financial decisions, and technological advances, people will also need to make lifestyle adjustments.

According to an IPCC study, everyday behavioural changes by people which reduce demand for energy – such as adjusting temperature settings in buildings and reducing air travel – can cumulatively lead to substantial reductions in carbon emissions. People across the world are increasingly concerned about climate change and want to do something about it. Climate change is inspiring people to step up to a higher cause, to take collective action for the common good of our planet.

Singaporeans too are becoming more environmentally conscious. According to a 2020 study by the Institute of Policy Studies, 61% of Singaporeans surveyed felt that protecting the environment should be prioritised even if it results in slower economic growth and some loss of jobs. More individuals are taking climate-friendly actions, motivated by a desire to preserve a liveable world for future generations.

There are many things we can do as individuals to minimise our impact on the climate.

We can do energy audits of our homes to identify ways to be more energy efficient.

We can reduce food and plastic waste. We can become a zero-waste nation and a circular economy, where we use less resources and re-cycle resources. We can eat lower in the food chain and shift towards more plant-based protein. University of Oxford researchers have found that reducing meat and dairy products from our diet can help to shrink our carbon footprint from food by up to 73%.

We can drive less and take public transport more. According to a 2021 study of seven European cities, individuals who switched one trip per day from driving to cycling reduced their carbon footprint by about 0.5 tonnes over a year.

CONCLUSION

Let me conclude. This is a gathering in the name of the dismal science. I hope I did not give too dismal a speech. But it is important that as economists and as Singaporeans, we appreciate the gravity of the net zero challenge.

The climate crisis demands collective action: nothing short of a whole-of-society effort across countries will suffice. And the time for action is now, not tomorrow. Yes, we wish we can postpone carbon taxes, costly investments in energy efficiency, restructuring of business processes, mandatory reporting of climate risks, until economic conditions are better. But the planet cannot wait, it is continuing to warm up. The cost of delay is having to make sharper and more painful adjustments later amid a worsening climate.

The road to net zero is not easy. But we have seen time and again that when confronted with grave challenges, humankind has risen to the challenge. The recent COVID-19 pandemic is a good example. Yes, the world's response was not optimal, and not everyone played their part. But by and

large, governments put in place the necessary measures to save both lives and livelihoods; scientists and industry came together to produce vaccines in record time; businesses adapted and changed to continue providing goods and services; and people around the world took the necessary precautions, adjusted to new ways of living and working, made sacrifices, and helped one another out.

With that same spirit, difficult as it may be, the world will get to net zero and avert climate disaster. It will be a better world, and a better Singapore.

To read more:
https://www.mas.gov.sg/news/speeches/2022/what-does-it-take-to-get-to-net-zero-keynote-speech-by-mr-ravi-menon-managing-director-monetary-authority-of-singapore-at-the-economic-society-of-singapore-annual-dinner-2022-on-17-august-2022

Number 9

Ransomware: Publicly Reported Incidents are only the tip of the iceberg

The threat landscape report on ransomware attacks published today by the European Union Agency for Cybersecurity (ENISA) uncovers the shortcomings of the current reporting mechanisms across the EU.

As one of the most devastating types of cybersecurity attacks over the last decade, ransomware has grown to impact organisations of all sizes across the globe.

What is ransomware?

Ransomware is a type of cybersecurity attack that allows threat actors to take control of the assets of a target and demand ransom for the availability and confidentiality of these assets.

What the report covers

This threat landscape report analysed a total of 623 ransomware incidents across the EU, the United Kingdom and the United States for a reporting period from May 2021 to June 2022. The data was gathered from governments' and security companies' reports, from the press, verified blogs and in some cases using related sources from the dark web.

The findings and what they tell us

Between May 2021 and June 2022 about 10 terabytes of data were stolen each month by ransomware threat actors. 58.2% of the data stolen included employees' personal data.

At least 47 unique ransomware threat actors were found.

For 94.2% of incidents, we do not know whether the company paid the ransom or not. However, when the negotiation fails, the attackers usually expose and make the data available on their webpages. This is what happens in general and is a reality for 37,88% of incidents.

We can therefore conclude that the remaining 62,12% of companies either came to an agreement with the attackers or found another solution.

The study also shows that companies of every size and from all sectors are affected.

The above figures can however only portray a part of the overall picture. In reality, the study reveals that the total number of ransomware attacks is much larger. At present this total is impossible to capture since too many organisations still do not make their incidents public or do not report on them to the relevant authorities.

Information about the disclosed incidents is also quite limited since in most cases the affected organisations are unaware of how threat actors managed to get initial access. In the end, organisations might deal with the issue internally (e.g. decide to pay the ransom) to avoid negative publicity and ensure business continuity. However, such an approach does not help fight the cause – on the contrary, it encourages the phenomenon instead, fuelling the ransomware business model in the process.

It is in the context of such challenges that ENISA is exploring ways to improve this reporting of incidents. The revised Network and Information Security Directive (NIS 2) is expected to change the way cybersecurity incidents are notified. The new provisions will aim to support a better mapping and understanding of the relevant incidents.

What can Ransomware do: the lifecycle and the business models

According to the analysis of the report, ransomware attacks can target assets in four different ways: the attack can either Lock, Encrypt, Delete or Steal (LEDS) the target's assets. Targeted assets can be anything such as documents or tools from files, databases, web services, content management systems, screens, master boot records (MBR), master file tables (MFT), etc.

The life cycle of ransomware remained unchanged until around 2018 when ransomware started to add more functionality and when blackmailing techniques matured. We can identify five stages of a ransomware attack: initial access, execution, action on objectives, blackmail, and ransom negotiation. These stages do not follow a strict sequential path.

5 different ransomware business models emerged from the study:

1. A model focused around individual attackers;
2. A model focused around group threat actors;
3. A ransomware-as-a-service model;
4. A data brokerage model; and,

5. A model aimed mostly at achieving notoriety as key for a successful ransomware business (ransomware operators need to maintain a certain reputation of notoriety, otherwise, victims will not pay the ransom).

The report recommends the following:

1. Strengthen your resilience against ransomware by taking actions such as:

- keep an updated backup of your business files & personal data;
- keep this backup isolated from the network;
- apply the 3-2-1 rule of backup: 3 copies, 2 different storage media, 1 copy offsite;
- run security software designed to detect most ransomware in your endpoint devices;
- restrict administrative privileges; etc.

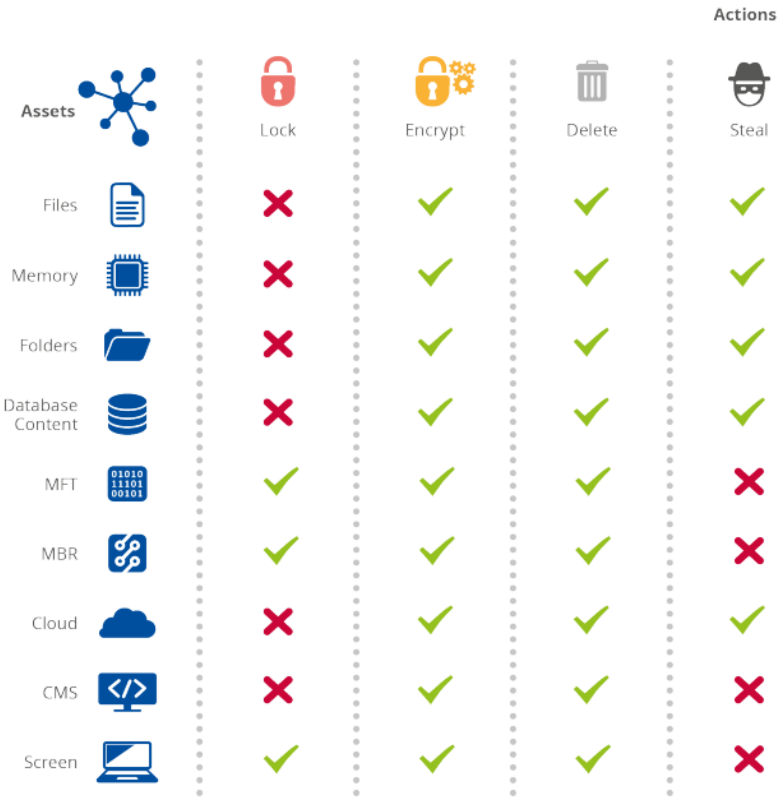
2. If you fall victim of a ransomware attack:

- contact the national cybersecurity authorities or law enforcement for guidance;
- do not pay the ransom and do not negotiate with the threat actors;
- quarantine the affected system;
- visit the No More Ransom Project, a Europol initiative; etc.

It is strongly recommended to share your ransomware incident information with your authorities to be able to alert potential victims, identify threat actors, support the security research and develop means to prevent such attacks or better respond to them.

Find out more in the report: ENISA Threat Landscape for Ransomware Attacks at:
https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks

Table 1: Capabilities of current ransomware in terms of actions they perform and assets they target



ENISA's work on the Cybersecurity Threat Landscape

Ransomware was already classified as a prime threat in ENISA's Annual Threat Landscape of 2021 and had consistently been considered among the prime threats in previous ETL editions.

This ransomware threat landscape report was developed on the basis of the recently published ENISA Threat Landscape Methodology — ENISA (europa.eu). The new methodology aims to provide a consistent and trusted baseline for the transparent delivery of horizontal, thematic and sectorial cybersecurity threat landscapes using a systematic and transparent process for data collection and analysis.

ENISA is constantly looking for ways to gather feedback and to continually improve and update the methodology applied to the performance of cybersecurity threat landscapes. Please feel free to reach out to etl@enisa.europa.eu with suggestions.

Target audience:

- European Commission and European Member States policy makers (including but not limited to European Union institutions (EUIs);

- EU institutions, bodies and agencies (EUIBAs);
- Cybersecurity experts, industry, vendors, solution providers, SMEs;
- Member States and national authorities (e.g. cybersecurity authorities);

To read more:
https://www.enisa.europa.eu/news/ransomware-publicly-reported-incidents-are-only-the-tip-of-the-iceberg

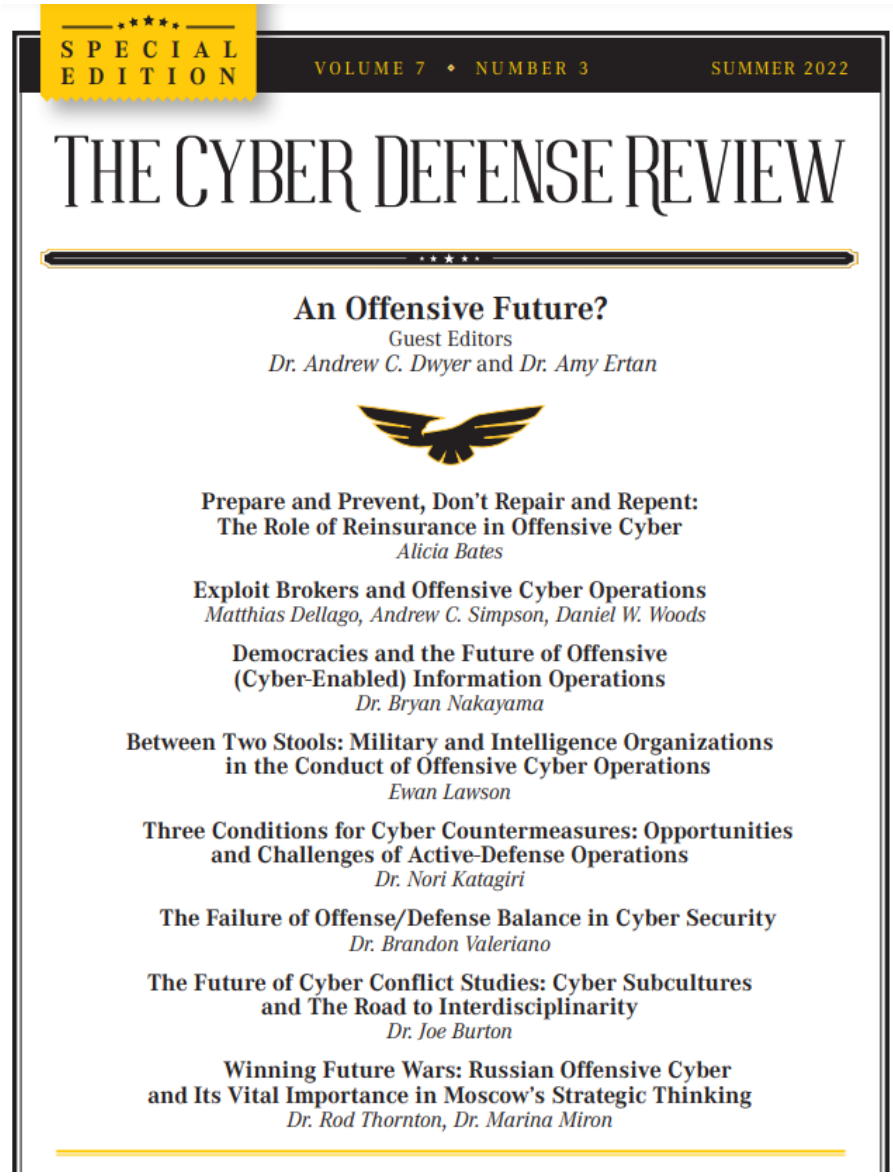
Number 10

The Cyber Defense Review
VOLUME 7, NUMBER 3, SUMMER 2022

THE CYBER DEFENSE REVIEW

You can read:

To read it:
https://cyberdefensereview.army.mil/Portals/6/Documents/2022_summer_cdr/CDR_V7N3_Summer_2022-SE-WEB-1.pdf?ver=oDnMjK7AGrLLtmFJPHUwxQ%3d%3d


SPECIAL EDITION

VOLUME 7 • NUMBER 3 SUMMER 2022

THE CYBER DEFENSE REVIEW

An Offensive Future?

Guest Editors
Dr. Andrew C. Dwyer and *Dr. Amy Ertan*

Prepare and Prevent, Don't Repair and Repent: The Role of Reinsurance in Offensive Cyber
Alicia Bates

Exploit Brokers and Offensive Cyber Operations
Matthias Dellago, Andrew C. Simpson, Daniel W. Woods

Democracies and the Future of Offensive (Cyber-Enabled) Information Operations
Dr. Bryan Nakayama

Between Two Stools: Military and Intelligence Organizations in the Conduct of Offensive Cyber Operations
Ewan Lawson

Three Conditions for Cyber Countermeasures: Opportunities and Challenges of Active-Defense Operations
Dr. Nori Katagiri

The Failure of Offense/Defense Balance in Cyber Security
Dr. Brandon Valeriano

The Future of Cyber Conflict Studies: Cyber Subcultures and The Road to Interdisciplinarity
Dr. Joe Burton

Winning Future Wars: Russian Offensive Cyber and Its Vital Importance in Moscow's Strategic Thinking
Dr. Rod Thornton, Dr. Marina Miron

Disclaimer

The Association tries to enhance public access to information about risk and compliance management.

Our goal is to keep this information timely and accurate. If errors are brought to our attention, we will try to correct them.

This information:

- is of a general nature only and is not intended to address the specific circumstances of any individual or entity;

- should not be relied on in the context of enforcement or similar regulatory action;

- is not necessarily comprehensive, complete, or up to date;

- is sometimes linked to external sites over which the Association has no control and for which the Association assumes no responsibility;

- is not professional or legal advice (if you need specific advice, you should always consult a suitably qualified professional);

- is in no way constitutive of an interpretative document;

- does not prejudge the position that the relevant authorities might decide to take on the same matters if developments, including Court rulings, were to lead it to revise some of the views expressed here;

- does not prejudge the interpretation that the Courts might place on the matters at issue.

Please note that it cannot be guaranteed that these information and documents exactly reproduce officially adopted texts.

It is our goal to minimize disruption caused by technical errors.

However, some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems.

The Association accepts no responsibility regarding such problems incurred because of using this site or any linked external sites.

International Association of Risk and Compliance Professionals (IARCP)

You can explore what we offer to our members:

1. *Membership* – Become a standard, premium or lifetime member.

You may visit:
https://www.risk-compliance-association.com/How_to_become_member.htm

2. *Weekly Updates* - Visit the *Reading Room* of the association at:
https://www.risk-compliance-association.com/Reading_Room.htm

3. *Training and Certification* – Become:

- a Certified Risk and Compliance Management Professional (CRCMP),

- a Certified Information Systems Risk and Compliance Professional (CISRCP),

- a Certified Cyber (Governance Risk and Compliance) Professional - CC(GRC)P,

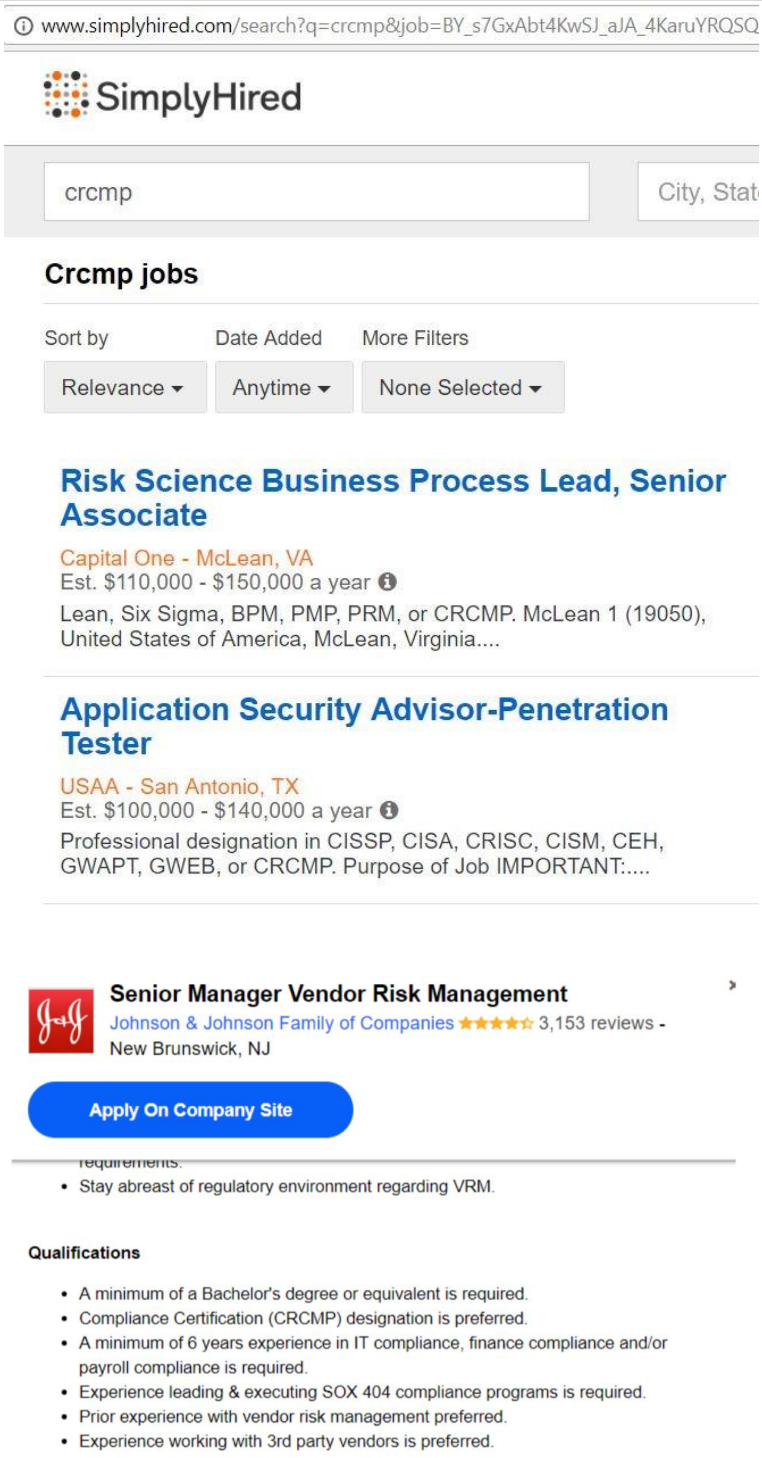
- a Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I,

- a Travel Security Trained Professional (TSecTPro).

The CRCMP has become one of the most recognized certificates in risk management and compliance. There are CRCMPs in 32 countries.

Companies and organizations around the world consider the CRCMP a preferred certificate:

Senior Information Security Risk Analyst
Public Company Accounting Oversight Board - ★★★★☆ 10 reviews - Washington, DC
Professional designation in CISSP, CISA, CRISC, or CRCMP preferred. The PCAOB is a nonprofit corporation established by Congress to oversee the audits of public...



You can find more about the demand for CRCMPs at:
https://www.risk-compliance-association.com/CRCMP_Jobs_Careers.pdf

For the Certified Risk and Compliance Management Professional (CRCMP) distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/Distance_Learning_and_Certification.htm

For the Certified Information Systems Risk and Compliance Professional (CISRCP), distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/CISRCP_Distance_Learning_and_Certification.htm

For the Certified Cyber (Governance Risk and Compliance) Professional - CC(GRC)P, distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/CC_GRC_P_Distance_Learning_and_Certification.htm

For the Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/CRCMP_Re_I.htm

For the Travel Security Trained Professional (TSecTPro), distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/TSecTPro_Distance_Learning_and_Certification.htm

Certified Cyber (Governance Risk and Compliance) Professionals - CC(GRC)Ps, have a 50% discount for the Travel Security Trained Professional (TSecTPro) program ($148 instead of $297).

You have a $100 discount after you purchase one of our programs. The discount applies to each additional program. For example, you can purchase the CRCMP program for $297, and then purchase the CISRCP program for $197 (instead of $297), the CC(GRC)P program for $197 (instead of $297), the CRCMP(Re)I program for $197 (instead of $297), and the TSecTPro program for $197 (instead of $297).

For *instructor-led* training, you may contact us. We can tailor all programs to meet specific requirements.