BCS the Chartered Institute for IT – Sri Lanka Section
Member News letter
Volume: 5, 2018

Editors' message

Dear Members,

We BCS Sri Lanka Section published a news letter on behalf of the SL Section as a mark of 20th year of BCS Sri Lanka Section. This is with the intention to communicate with the membership periodically and update the members on the activities carried out by the chapter. Currently we are releasing the 3rd newsletter for this year; we initially planned to release 2 newsletters for a year and gradually increase it up to 4 newsletters for a year. The support and encouragement given by the BCS Sri Lanka membership pushed us to fast-forward the target within 3 months. In addition all our releases are targeted towards a specific special interest groups, volume 1 focused on eCommerce & Internet, Volume 2 focused on Application Development & Management, Volume 3 focused on IT Security & Cyber Law, Volume 4 on Management and Volume 5 on GDPR.

Thank you very much for all the encouragement and appreciation shared in this regard through email and in all other means. We hope you will continue to support us on this initiative. Please send us your feedback to nirmalan@bcssrilanka.org we will try our best to keep up with it.

Message from the Section Chairman

The New Beginning With New Hope

BCS the Chartered Institute for IT Sri Lanka Section (BCSSL) successfully completed 2017 year with many activities. The New Year is started with the conclusion of the AGM and added energy to address the challenges affecting the Section members and the ICT industry at large.

The Section Committee has planned many projects to improve the benefits and professional development of the section members during this year. This would include multiple types of sessions to improve the skills and knowledge of members along with improved opportunity for networking among the members and Industry experts.

In addition, the section would conduct NBQSA the National Best Quality ICT Awards, its flagship event for the ICT industry in the country, Biz2Biz program which is the sections' Business support program for the Industry and YPG events extending to senior professionals and ICT industry.

The sub-committees which organize these activities require the support of many volunteers as resource persons and organizers. And BCSSL members who wish to do so are requested to contact the secretariat calling or sending an email.

Further, Executive committee wishes to request all BCSSL members to utilize these opportunities to get involved either as volunteers in organizing activities or as participants of these events to network with professionals, other members and other industry experts.

Executive Committee and I wish take this opportunity to wish you all the best for the year ahead and look forward to your involvement with the section activities!

Ruwan Amarasekara
Chairman – BCS the Chartered Institute for IT Sri Lanka Section

**All articles published on our newsletters, are with the permission of the authors and all the chairman 's messages are unedited.

BCS the Chartered Institute for IT – Sri Lanka Section
Member News letter
Volume: 5, 2018

Articles

European Union General Data Protection Regulation (GDPR): Things to be aware.

N Nirmalan

CEO/Principal Consultant, KenVisa.

In an era of digital transformation, heavy utilization of digital assets and services, digital marketing, big data etc creates a need for data capturing. Now a days captured data is stored in multiple forms, in multiple devices including handheld devices.

Data breaches do happen. Information gets lost, stolen or even released into the hands of people who were never intended to see it. Wherever personal data is collected, stored, used, and finally deleted or destroyed, privacy concerns rise.

Businesses are accountable for monitoring and protecting that data on an ongoing basis, to provide customers with trust and confidence, which is currently diminishing in businesses.

The European Union General Data Protection Regulation (GDPR) is a set of rules about how companies should process the personal data of data subjects. The European Union GDPR affects every organization, Big and small, that processes EU personal data. GDPR protects user data in just about every conceivable way. The GDPR operates with an understanding that data collection and processing provides the basic mechanism that most businesses run on, but it also attempts to protect that data every step of its way while giving the consumer ultimate control over what happens to it.

GDPR is the most strict regulation which has come out within the past few decades.

In order to be GDPR compliant, a company must not only handle consumer data carefully but also provide them with ways to control, monitor, check and, if desired, delete any information pertaining to them that they want.

GDPR lays out responsibilities for organizations to ensure the privacy and protection of personal data, provides data subjects with certain rights, and assigns powers to regulators to ask for demonstrations of accountability or even impose fines in cases where an organisation is not complying with GDPR requirements. Under the terms of GDPR, not only will organisations have to ensure that personal data is gathered legally and under strict conditions, but those who collect and manage it will be obliged to protect it from misuse and exploitation, as well as to respect the rights of data owners or face penalties for not doing so.

Companies that wish to stay in compliance must implement processes to ensure that when data is handled, it remains protected. There is also an opportunity for significant process improvement for those companies that standardizes the requirements for privacy and data protection, which will also increase the efficiency of the organizational performance and minimize the risk of non-compliance.

The GDPR was adopted by the EU Council and Parliament in April 2016, and will take effect in every EU member states from 25th May 2018.

Principles

GDPR outlines the six principles that should be applied to any collection or processing of personal data.

- Personal data must be processed lawfully, fairly and transparently.
- Personal data can only be collected for specified, explicit and legitimate purposes.
- Personal data must be adequate, relevant and limited to what is necessary for processing.
- Personal data must be accurate and kept up to date.
- Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.
- Personal data must be processed in a manner that ensures its security.

The data controller is responsible for demonstrating this, and they must secure the same assurances from any external data processors with whom they contract.

The processor is a person or an organization that process the data on behalf of the controller. The controller is a person or an organization who determine what happens to the personal data

Applicability

The GDPR applies to organisations within the European Union (EU), and to any external organisations that are trading within the EU. It also covers other residents of the EU, including refugees, people on work and travel visas, those with residency, and so on, and could also be applied to non-EU residents whose personal data is held and/or processed within the EU. At the same time it has not distinguished between data subjects on the basis of nationality or location.

GDPR states that both the data controller and the data processor are liable in the event of a data breach.

The GDPR states that the personal data is any information relating to an ''identified or identifiable natural'' person ("data subject"); that is a person who can be identified by a unique identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

This extended list indicates that the data commonly used, may no longer be suitable for distribution or sharing in public. Therefore any information that could be used to identify the data subject should be subject to the same protections.

Repercussions

Certification bodies involved in certification schemes in accordance with the Regulation, can face fines if they do not comply with their responsibilities. The data controller, any number of data processors involved in the data breach, the certification body that approved the data processing, all can be penalized if they are found to be guilty.

Since the administrative penalties can be applied so broadly, it is very important to understand what your obligations and exposure are. It is also important to remember that these penalties are in addition to any other fines or legal costs that you may incur following a data breach.

For some of the breaches in the regulation, the fines can go up to 20 million Euros or 4% of the global annual turnover, whichever is greater.

Data subjects' rights

The expanded rights granted to data subjects, will give them more control over their data and give them a better understanding of what is being done with it.

- The right to be informed

  GDPR states the information you should provide and when individuals should be informed. The right to be informed encompasses your obligation to provide 'fair processing information', typically through a privacy notice. It emphasizes the need for transparency over how you use personal data. The information you supply about the processing of personal data must be: concise, transparent, intelligible and easily accessible, written in clear and plain language, particularly if addressed to a child; and free of charge.

- The right of access

  Individuals have a right to know what personal data of theirs is being stored and how it is being processed. They can also ask for their data to be corrected if it is wrong. There is now also a requirement for data portability, meaning individuals can request their data to be delivered in a structured and commonly used file format, so that it can be transferred to some other organisation.

- The right to rectification

  Data subjects are entitled to have personal data rectified if it is inaccurate or incomplete.

- The right to erasure

  Also known as ''right to be forgotten'' gives the data subject the right to request the deletion or removal of the personal data where there is no requirement for continued processing. Individuals may withdraw their consent to processing their data at any time, and ask the data controller to erase their personal data. This must be done without undue delay. Data controller must take reasonable steps to inform third parties to remove any copies of that data held with them. It is quite likely that the data protection authority in your country will still want to see that continued effort has been taken to ensure that all appropriate technical and procedural measures to erase the data have been employed.

- The right to restrict processing

  GDPR rules that personal data shall only be stored and processed to the extent where it is necessary to the explicit purpose for which the data was originally collected. Data shall also not be stored longer than is necessary, which means many organisations will need to take a good, hard look at their Big Data programs. Also individuals can also restrict processing their data to certain purposes such as direct marketing.

  Data subject has the rights to restrict the processing, where you are permitted to store the data, but not further process

it. This ensures retainment of just enough information about the individual to respect the restriction is respected in further.

- The right to data portability

  The right to data portability allows data subjects to request a copy of any personal data held on them, and reuse their personal data for their own purposes across different services.

  It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. Also request that this information is transmitted to another data controller.

- The right to object

  Data subjects have the right to object to processing unless the controller demonstrates compelling legitimate grounds for processing. Where personal data is processed for direct marketing purposes, data subjects have the right to object at any time to the processing.

- Rights in relation to automated decision making and profiling.

  Data subjects have the right not to be subject to a decision based solely on automated processing, including profiling, unless the data subject has given explicit consent, or where the processing is authorized by contract or in law.

GDPR has increased the rights of data subjects. From the organization's point of view, this means that it will need to ensure that is clear about what data that it is collecting and what it will be using it for.

If data subjects believe that their rights are breached, they will be able to seek judicial remedies against controllers and processors, and will also have the right to seek compensation from them for the damages arising from breaches of the GDPR. They also have the right to lodge a complaint with their relevant data protection authority if GDPR is believed to be breached.

Consent

The data subject's consent means any freely given, specific, informed, and unambiguous indication of the data subject's wishes to process personal data. In addition for special categories of personal data such as health, genetic, racial or ethnic, sexual orientation, political opinions, biometric etc, will need explicit consent from data subject, as processing of these data is prohibited.

Data controllers will have to ensure that they secure clear and unambiguous consent from the data subject before processing personal data. Processing cannot proceed unless the data subject has consented to every processing activity. Children under 16 are also no longer able to consent to having their personal data processed.

GDPR requires that the consent document be laid out in simple terms, should be clear, concise and not be conditioned. Documentation of consent is important as the withdrawal of the consent and there should be easy ways laid out for this process.

Lawful processing

Controllers are accountable for ensuring that personal data is lawfully, fairly and transparently processed.

Personal data can only be processed for limited purposes, to a minimal extent and accurately. This ties into the requirement for transparency: the data subject must be aware of the nature of the processing, which will inform the 'limited purposes' and 'minimal extent'.

Retention of data

Personal data can also only be retained for limited periods, which should be clear to the data subject at the point at which they consent. Regardless of the length of the retention confidentiality and integrity must be secured, including against accidental loss, destruction or damage. This is very important and should be an extremely high priority and the organizations suppliers and partners also understand and implement this.

The "one-stop shop"

The Regulation is intended to be a single scheme, applied consistently across the EU in order to maintain a common market and support the free flow of information.

Each state will determine a number of supervisory authorities or data protection authorities, who will be the local point of contact for all GDPR issues. This is the "one-stop shop" mechanism, which is intended to reduce the bureaucratic load involved in dealing with potentially complex issues. Each state will also determine a lead supervisory authority or data protection authority, which will appoint a member to the EU Data Protection Board described above.

non-unitary states may choose to operate these authorities on a regional basis, with a lead supervisory authority established at the national level. Organisations processing personal data across a number of EU member states will deal with the data protection authority in their primary jurisdiction.

Data controllers are regulated by a lead authority located in the territory of their main establishment, although local authorities may deal with local cases. If a concerned supervisory authority objects to a lead authority's draft decision, the case shall be referred to the consistency mechanism for a binding decision by the European Data Protection Board. Any European Data Protection Board binding decision can be appealed to the Court of Justice of the European Union.

Records of data processing activities and Documentation

GDPR requires every data controller to retain a record of its data processing activities. This record needs to contain a specific set of information such that it is clear what data is being processed, where it is processed, how it is processed and why it is processed.

Data processors are also required to keep records of all processing carried out on behalf of a data controller. These records need to be made available to the supervisory authority on request.

In addition to the explicit and implicit requirements for the maintenance of specific records, should able to demonstrate

that you have documented/evidence that best practices are consistently applied, that you have an audit trail showing that you notified the required authorities and any affected data subjects within the required timeframes, and that you have taken all the appropriate steps to mitigate the impacts of the data breach. Including, proof of consent from data subjects.

Data protection impact assessments

Data Protection Impact Assessments (DPIAs) are now mandatory for technologies and processes that are likely to result in a high risk to the rights of data subjects.

This includes processes, not just applications, if any of the processes concerned resulted in a loss of data protection, and the organization have not addressed this "by design and by default", then the organization is likely to be held liable in the event of a data breach.

In line with the data protection by design and by default strategies, organisations should ensure that a DPIA is part of their risk assessment process regarding personal data, and data controller is responsible for ensuring that DPIAs are conducted.

Controller/processor contracts

When it come to controller outsource/contracts with a processor to process personal data, the processor should provide significant guarantee that adequate security measures (including technical and organizational) will be complied according to GDPR requirements in protecting the rights of the data subjects. If the processor requires contracting another processor for the same requirement, the same guarantee should be given by the second processor and this cannot happen without the authorization of the controller.

Contractual arrangements are reviewed and updated to ensure that responsibilities and liabilities between the controller and processor are stipulated as per requirements. At the same time the data controller is held accountable for failures of any data processor.

Data breaches

As part of best practice there should be processes in place to make notifications in the event of a data breach. Data breach reports must be made within 72 hours of the data controller becoming aware of the breach. If the breach suppose to result in a high risk to the rights and freedoms of data subjects, they must be contacted "without undue delay".

Encryption, Cookies and IP Address

It is a legal requirement that all cryptography modules must be Federal Information Processing Standard (FIPS) 140 compliant. Encryption should be applied to storage of personal data, and for establishing secure connections when personal data is transmitted.

The GDPR itself mentions cookies as an online identifier, which means it is considered as personal data and, therefore, the data subject must consent. Therefore all of the cookie notifications will need to follow the normal rules for consent, but there are exemptions for this under certain conditions.

GDPR consider cookies and IP addresses to be personal data. Also states that organizations that use IP addresses to do anything other than deliver content need to ensure that consent is sought and gained.

International transfers

The GDPR deals specifically with situations where a controller or processor intends to transfer personal data outside the EU. Such international transfers are only legal if they comply with the conditions stated in GDPR. These conditions require specific safeguards to be in place, including on the basis that data subject rights and effective legal remedies are available.

International transfers can only take place if the controller or processor has put in place legally binding and enforceable arrangements to protect the rights of EU data subjects. As the controller and processor are accountable for the personal data they are processing, any agreement to transfer that data to a third party, outside the arrangements identified in the GDPR, will be illegal. This is particularly important when considering Cloud providers. It is important to keep in mind that regulations covering international transfers are subject to the highest administrative penalty.

Conclusion

GDPR has come in to place as a savior for the long frustrated data owners, who were affected/ ignored by the corporate, who have not given sufficient considerations for privacy and protection for the personal data. This big hope of privacy can only see the light if it is implemented without compromise, which we will have to wait and see the success of it

This regulation has turned many things to relook at, including the current hypes such as big data, data analysis, digital marketing, multi sourcing etc. where personal data is compelled to given consideration more seriously than ever before.

Organizations also need to review various contracts with third parties in ensuring that service-level agreements, procurement, outsourcing processes, are reviewed in line with the requirements of the GDPR. In addition, also need to check your suppliers of Cloud services, remote servers etc in line with this.

In addition organizations need to relook at the process, procedures and contracts in handling personal data, in line with GDPR to avoid non compliance and threatening penalties. This will also create a need for educating the personal data handlers and competent staff in taking this forward successfully.

Source: EU GDPR

Implement & institutionalize GDPR requirements by leveraging COBIT, ITIL & ISO 27001.(This iarticle was published in Linkedin on 1Mar18)

Rajiv K Dua

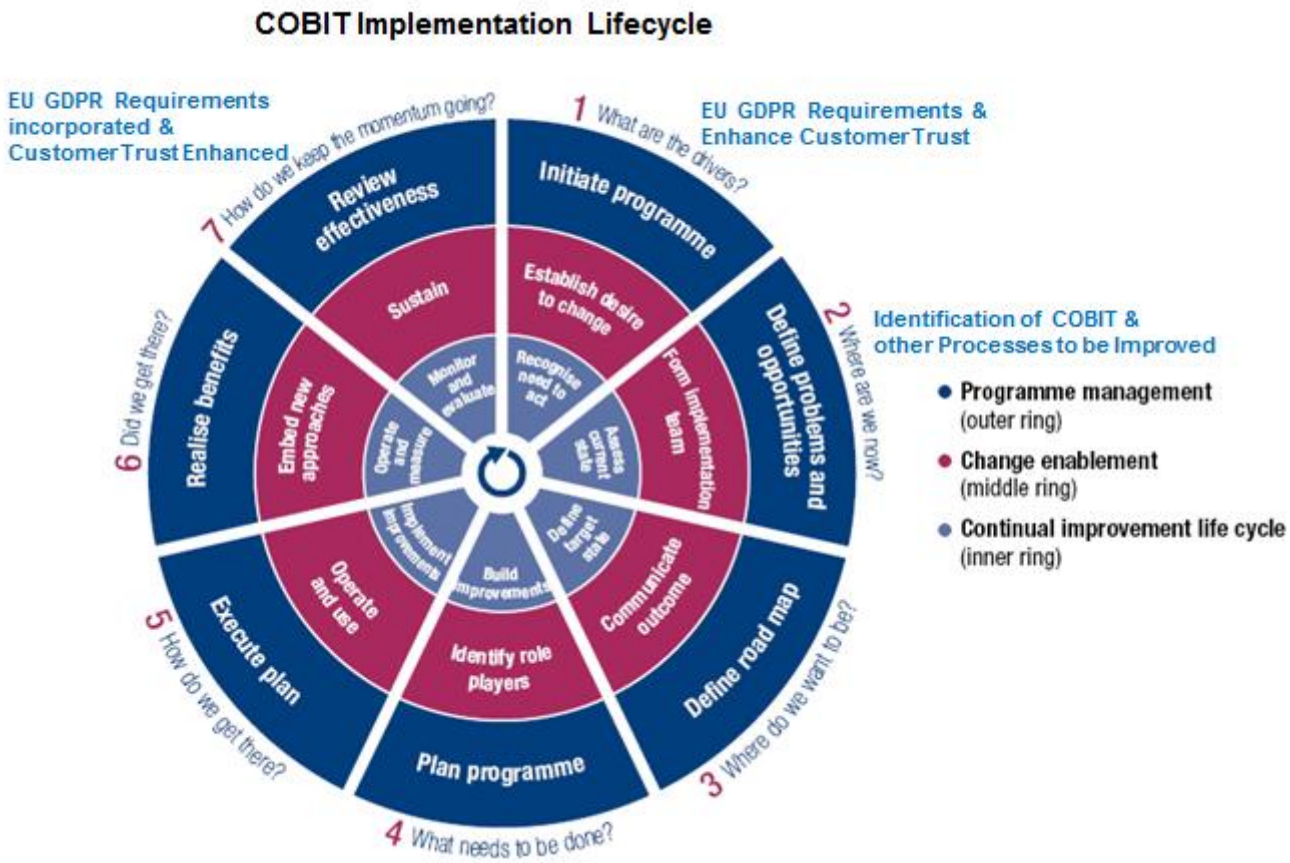
IT Consultant & Accredited Trainer for COBIT, ITIL, DevOps, BRM, Cloud, Agile Service Management, ISO 20000.

In today's ever evolving digital environment, the protection of personal data has become more critical than ever. To mitigate dangerous and costly consequences that often come with online data, which is getting collected and often without proper and explicit consent from the Data Subjects, European Union has approved General Data Protection Regulation (GDPR). Once it comes into force from 25 May 2018, it will give data subjects(Customers, Employees & Suppliers) of all the 28 EU member states significant new rights over how their personal data is collected, processed and transferred by data controllers and processors. It demands significant data protection safeguards, more stringent reporting requirements and significantly higher penalties than has been the case previously and organizations will need to have a number of new processes & organization roles in place in order to meet these requirements.

With the heightened restrictions imposed by the GDPR, the EU aims to renew the public's trust in the ever-developing digital arena. Organizations should not implement GDPR as a compliance burden but rather embrace it with a positive objective of enhancing the trust with the Data Subjects and use it as a competitive advantage. GDPR should not be seen & implemented as a mutually exclusive project, rather it should be seen as new stakeholders need to be incorporated in the existing Governance and Management systems. COBIT, globally acceptable & defacto industry standard Business framework for the Governance & Management of Enterprise IT, provides best practice guidance built on Five Principles & Seven Enablers to incorporate this new requirement in an institutionalized way. Using the **COBIT Goals Cascade**, GDPR requirements like any other compliance SOX, HIPPA or business performance requirements can be cascaded to Enterprise goals to IT-related goals to Enablers goals. Processes identified through this goal cascade and other required enablers can thereafter be modified to implement this change, along with other regular stakeholder needs using COBIT Implementation life cycle approach.

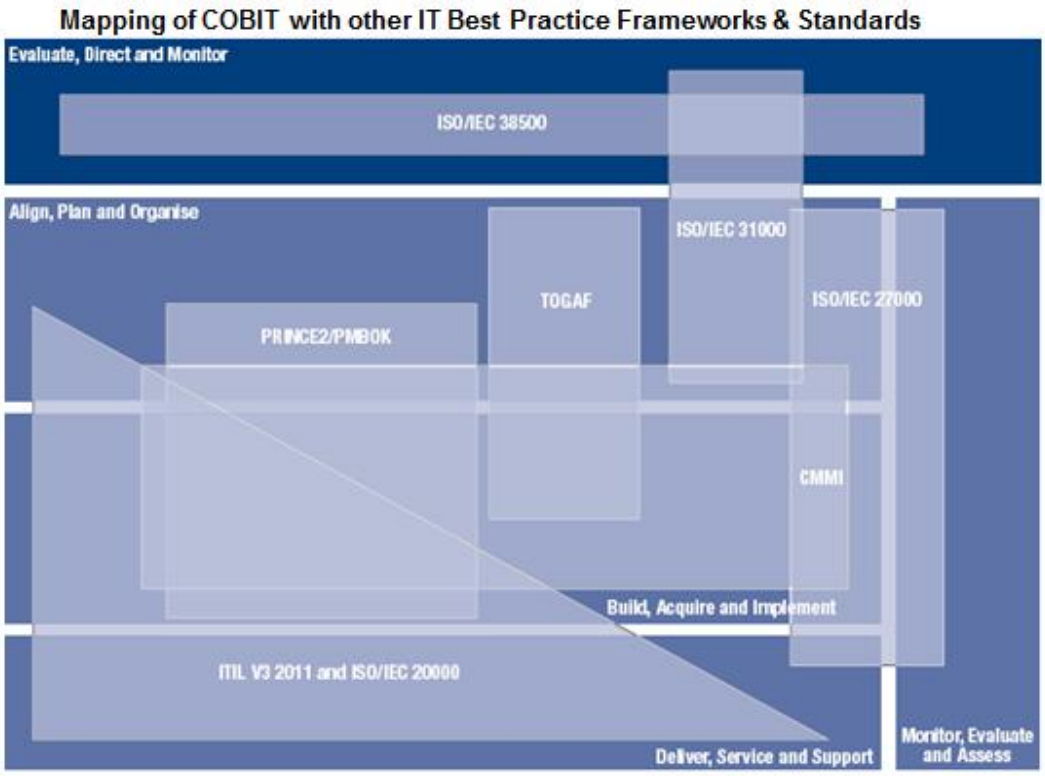
Goal Cascade Image.

COBIT Implementation guidance provides structured and detailed guidance to implement & institutionalize any new stakeholder need(GDPR etc.), using a life cycle approach split into seven phases and each phase involves activities related to Program Management, Identified Improvements & Organizational Change Management (an integral & very important part of such initiatives).



Cobit Implementation Lifecycle Image

COBIT provides high level guidance for Business performance and conformance and integrates effectively with other frameworks & standards like ISO 27001, ITIL, TOGAF, ISO 31000 etc. for detailed guidance. COBIT Mapping with other IT Best Practices & Standards is shown below. COBIT acting as a single overarching & integrator framework, creates a simple architecture for structuring guidance in a non-technical, technology agnostic & common language for all the required stakeholders to work on such initiatives as a Business project. To comply with GDPR, we will have to make changes largely in COBIT processes, ISO 27001 (ISO 27002, ISO 27017, ISO 27018 as applicable) & ITIL processes. Besides Process, changes would be required in other enablers like Technology Infrastructure, Applications, Organization structure, People Skills (Training), Culture etc.



Any organization which has mature COBIT, ISO 27001 & ITIL Service Management Systems, are more than half way through incorporation of GDPR requirements already. Shortcut/Band-Aid/Checklist approach will at best lead to implementation of GDPR as a costly project with diminishing returns thereafter.

In the Digital era, Business & Technology changes would be much more frequent than we have ever seen before and also applicability of EU GDPR in not restricted to EU based companies only but it applies to all companies across the globe that cater to EU Data Subjects. While EU has taken a lead to build confidence of Data Subjects in the Digital era, I foresee similar regulations coming up in other geographies too. There are already more than 15 countries (Norway, Iceland, Argentina, Canada, New Zealand, Switzerland, Israel etc.) outside of the 28 EU member states that have data protection laws in-line with requirements of the EU GDPR. Many countries including India need to expedite revision of the IT related laws to achieve their Digital Vision to stay globally competitive and from a corporate perspective we must follow structured governance & management approach and leverage IT best practices for such needs.

In my last COBIT Implementation workshop, we used EU GDPR as a new stakeholder need to be incorporated to achieve the value creation objective and identified processes in COBIT, ISO 27001 & ITIL which may need to be modified. The participants were extremely excited and worked till late in the evening for this mapping exercise. As we wrapped-up the workshop, the only worry they had was, how they will get their Top Management excited for the support needed for compliance initiatives like GDPR. I intend to post a short article in the coming week about my advice to them, which I shared as we walked towards the Car Parking.

**All articles published on our newsletters, are with the permission of the authors and all the chairman ‘s messages are unedited.

NBQSA The National Best Quality ICT Awards– New Challenges and future of Sri Lankan ICT industry

NBQSA The National Best Quality ICT Awards, is started by BCSSL in 1998 and this year we celebrate 20th Anniversary of NBQSA. Objectives of NBQSA is to benchmark Sri Lankan ICT Products with international standards and to give them the due recognition in Sri Lankan ICT market. In this view, NBQSA uses APICTA (Asia Pacific ICT Alliance) criteria to evaluate all competing products. NBQSA is the only National level competition that is available in Sri Lanka for the ICT industry.

World is moving in to a digital era with the introduction of IoT (Internet of Things), RPA (Robotic Process Automation), crypto currency and so on and so forth. New technological innovation that is blooming up within the ICT industry will be our new challenges. These upcoming changes in the industry will be setting up a new dimension for the objectives of NBQSA in future. We shall be geared up to welcome; these industry advancement with positive mind for a better tomorrow.

From this year onwards APICTA (Asia Pacific ICT Alliance) has decided to introduce an improved version of evaluation criteria in to the global competition. In accordance with that, NBQSA evaluation criteria will also be enhanced with effect from 2019 onwards.

NBQSA is not project that can be managed single handedly. It is project where you need to put in lots of team efforts. Therefore, I cordially invite all of you our BCS members to join hands to take NBQSA to greater heights. Currently NBQSA is the flagship event of BCS, but in future I would like to see NBQSA as the flagship event of our country. We all as ICT professionals and as IT practitioners can do a lot to make this dream come true. Future of the entire will be a knowledge base economy where knowledge will become your wealth. In this era yet to be dawn, compulsorily ICT would be playing a vital role. Imagine the demand that will be created and lest get together to take mother Sri Lanka to glow as a proud nation in the world. I see NBQSA as a golden opportunity for this futuristic vision.

Finally, I would like to highlight a quote from a world-renowned gentleman, Warren Buffett, ***"It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently."*** NBQSA has gained its reputation locally and internationally during the past 20 years. Now it is up to us to take it to greater heights without ruining it. So let's act together and do it right to make NBQSA shines brighter in future to come.

Sanjeeva Perera

Chairman NBQSA, 2018

Upcoming Activities

Period	Event Description	Scheduled Dates
March-May	NBQSA Awareness Sessions	In Progress
May	NBQSA Launch	10/May/18
May-June	Call for Applications	10th May Onward
May-June	Judges Nominations	1st week of June
June	Judges' Briefing	3rd week of June
June	Applications Close	30h June
July	Nominees' Briefing	6th July
July	Judging process (Commercial)	12th & 15th July
July	2nd Round evaluations (Commercial)	21st – 22nd July
August	Judging process (Tertiary)	4th & 5th August
August	2nd Round evaluations (Tertiary)	11th & 12th August
September	Lifetime achievers & Special Awards Evaluation	31st August

- 20th National Best Quality ICT Awards (NBQSA) will be held on 19th Oct 2018 at Galadari, Colombo Sri Lanka
- APICTA 2018 will be held in China from 9th October 2018.