HOW SMP CAN AUGMENT USING TECHNOLOGY

2021

AJA

#NEWTHINKING

Contents

AJA #NEWTHINKING

AJA #NEWTHINKING

AJA #NEWTHINKING

AJA #NEWTHINKING

Objective

Technology is the language of Business which facilitates enterprises by providing Products and Services to their Customers.

Practitioners (CA,CS,CMA,etc.) as Knowledge Workers empower enterprises to run businesses by providing assurance, compliance, and consulting services to their clients.

The Right Technology Infrastructure provides a strong platform for Practitioners (CA,CS,CMA,etc.) to use their professional skills more effectively and efficiently.

This book will provide a strategic roadmap on how to design and build the right technology platform for SMPs Firms to implement IT successfully as required and enable them to operate as virtual offices to serve clients from anywhere and anytime.

Technology is all pervasive and is impacting both enterprises and professionals, personally and professionally. This is increasingly becoming more relevant now, more than ever. It has become imperative for Practitioners (CA,CS,CMA,etc.) to use technology; either we do it strategically or an ad hoc basis. If we adapt technology strategically, we need to be proactive and look at automation of all critical processes so that services can be delivered to clients by partners/owners/staff of the firm operating from anywhere (remotely from home, client office or their homes). This will also enable SMPs Firms to be more productive/effective. This will also open-up innovative ways of providing services to clients anywhere, anytime by existing/new set of employees who could be working from anywhere. Technology can be used to integrate and standardise service deliverables and empower SMPs Firms as team of knowledge workers. Technology can thus not only to simplify our work but also amplify what we do with our time and competencies.

The current challenges of covid pandemic is causing unexpected economic and financial hardships to every sector of the economy including enterprises and professionals. This has differentiated enterprises based on their enabling IT Infrastructure and processes. The impact on SMPs Firms has also been based on how much of automated processes the SMPs Firms have implemented. Greater the automation, lesser has been the impact on delivery of services. SMPs Firms which are using IT extensively have been quick to adapt to changing challenges of lockdowns and still deliver services by enabling staff to perform their work remotely. This has clearly proven that SMPs Firms have to invest in IT in a structured and strategic way to ensure delivery of services.

The book provides the concepts and practice at a macro and strategic level for SMPs Firms. They can go back to the drawing board, re-look at the services they provide and the way they provide their services. Based on the envisioned future, they can use guidance in this book to design appropriate IT strategy to achieve goals as planned. SMPs Firms although common in their vision to serve their clients are unique in their own way due to diversity of knowledge, skills, systems and processes, services, type of clientele, operating environment, etc. This book can enable SMPs Firms to translate their vision into strategy, convert the strategy into specific IT initiatives and then identify right technology solutions to implement. This is done by using technology as the backbone for providing services to clients with the design of a virtual office so that all stakeholders can operate effectively and efficiently.

1. Scope

Technology delivers best results when backed with robust processes and systems. Use this book to identify processes to standardise and then automate to deliver standard offering of services. Whatever be the stage of technology deployment in your firm, primary or advanced, this book can be used as useful reference guide to relook at how your firm is using technology and then take it to level where you can operate the firm as a virtual office. The guidance here can serve as a roadmap to enhance use of technology. The best approach to use this book is to use it to design your digital strategy as appropriate and then prepare IT implementation plan covering specific service areas, timelines, milestones and deliverables. We are sure this book will prove to be extremely useful to prepare their digital roadmap and be future-ready.

SMPs Firms could be of various sizes and the value and volume of services they provide could vary. However, this book has been written from a generic perspective so that SMPs Firms could pick and choose and adapt what is relevant for them. You could use this book as a strategic roadmap to design how IT is deployed within the SMPs Firms. Please use this book to:

1. Get an understanding of how IT strategic planning is a key enabler for SMPs Firms.
2. Prepare a strategic road map for your firm as per your vision.
3. Identify how to benchmark current status of IT implementation and plan the road ahead in line with the overall strategy.
4. Choose specific technology tools as relevant and deploy them.
5. How to implement technology safely and securely by adapting security policy.
6. Select and use relevant templates and checklists for using technology effectively.

The objective of this publication is to provide not to provide guidance on the operational aspects of what technology to use but to focus on overall strategy the SMPs Firms have to adapt in implementing the right level of technology from a long-term perspective.

This publication provides a strategic roadmap for planning and implementing technology as per vision, mission and goals of the firm. It has five sections:

Section I: Provides an overview of how IT Strategic plan can be designed and implemented.

Section II: Provides guidance on how to prepare specific IT Road map for implementing IT as per Firm's Mission/Vision using guidance from DCMM 2.0 Model of ICAI.

Section III: Provides guidance on Identifying and evaluating specific IT solutions as relevant.

Section IV: Provides guidance on Technology Deployment including FAQs on Technology for SMPs Firms covering different areas of Technology deployment

Section V: Provides Sample checklists, templates and useful references to enable SMPs Firms to operate as Virtual office and be future-ready.

Please note that the guidance provided in this book is not comprehensive but could be a good starting point to move forward in your digital journey. Technology innovation happens at a rapid pace and by the time you read this, there may be newer and better solutions to implement. However, the strategic approach for planning IT implementation will remain relevant. SMPs Firms can prepare their own roadmap as applicable to them.

I. How to Develop Strategic Roadmap for SMPs Firms?

1. Introduction

Every stakeholder of SMPs Firms including partner/owner/manager and staff must become IT savvy. Practitioners (CA,CS,CMA,etc.) are knowledge workers but in this digital age, the power of this knowledge can only be harnessed when complemented with requisite IT skillsets. This makes it imperative to learn/update IT skills as appropriate for providing assurance, compliance, or consulting services. There are no ready-made solutions/training courses which can meet all the requirements of SMPs Firms. The senior management of SMPs Firms must perform SWOT analysis in this area and chalk out the strategy for updating IT skills to be able to deliver services and remain relevant in these challenging and uncertain times. IT strategic planning and IT planning could enable SMPs Firms to successfully unleash the power of technology to meet challenges and operate virtually. This will empower SMPs Firms which have the right IT infrastructure to provide services to clients anywhere/anytime by staff working from anywhere/anytime.

2. Need for IT Strategy

The covid crisis has already had an amazing effect as it has fast-forwarded technology adaption by SMPs Firms by at least five years. The use of technology has skyrocketed with most of the staff working at home, and Practitioners (CA,CS,CMA,etc.) firms and their staff have found ways to communicate with each other and continue to work during this crisis. However, the effectiveness is based on how well technology is deployed in the SMPs Firms and how quickly they innovated and implementing technology.

This pandemic has demonstrated how IT has become all pervasive and critical. This uncertain operating and working environment has shown that chartered accountants whether they are self-employed or employed in enterprises, and regardless of their age, experience, or expertise have to learn to use technology as relevant. IT has had tremendous impact on the way SMPs Firms performed and provided services during this crisis. It is needless to emphasise that using IT effectively enhances productivity. It is predicted that in most Practitioners (CA,CS,CMA,etc.)es, if SMPs Firms are not able to understand and use IT effectively, they will be relegated to areas which are less remunerative and more man-power intensive.

The challenge posed by IT is also an opportunity which can be leveraged by Practitioners (CA,CS,CMA,etc.) to enhance their contribution and provide services to clients from anywhere by staff who operate from anywhere. IT is a resource and a tool like any other and can be deployed for faster development of practice/career by making it an integral part of our internal competency. It is critical to consider investment in building the right IT infrastructure from a strategic perspective to harness value from this investment and achieve required deliverables.

3. What is a Strategic Plan?

Enterprises and SMPs Firms need a new strategic vision to survive and thrive in this digital era.
Strategy is defined as the long-range blueprint of an organisation's desired image, direction and destination what it wants to be, what it wants to do and where it wants to go. Strategic planning is a critical element for articulating a shared vision, and for building the necessary

framework necessary to work together on common goals. A good strategic plan will provide clarity on how strategic goals will be achieved. It outlines long-term goals and details the specific strategies and goals that are to be pursued. The strategic planning process has to be iterative and provide a roadmap for transition from the present situation to the future vision.

The Strategic Plan must be a living document and should be re-visited to review accomplishments against set objectives, so that feedback is provided that will influence future planning and decision making.

4. Importance of IT Strategy Plan

IT strategy plan can help SMPs Firms to assess the status of their IT resources, competencies, skills, and capabilities to as to map it with vision of the firm. Developing a comprehensive plan is essential for SMPs Firms of all sizes to achieve sustainable goals. The risks of not developing a strategic plan is that it leads to complacency, severe impact of operations due to uncertain events, hampers future growth resulting in failure to deliver services for existing and future clients. Hence, it is imperative to give top priority for designing and developing a IT strategic plan for the firm. Information Technology (IT) is key enabler for enterprises and human resources are most critical for management of IT. The Principal/ Senior partner of the firm has to ensure that the right type of organisation structure is set up depending on the nature of services, type of technology deployment and objectives of client deliverables so as to ensure that firm's overall goals are achieved efficiently and effectively.

5. Key Strategy issues

The key issues to be considered in designing and developing a strategic plan for SMPs Firms are:

1. Who are we as a firm?
2. What does our firm want to be known for?
3. Where are we now in our growth strategy?
4. Where do we want to be in future and why?
5. What needs to be done to get there and how?
6. How do we know when we get there?
7. How do we implement required processes and systems to deliver services to reach our goals?
8. What type of IT infrastructure and investment is required to empower the firm and its employees to achieve required services and at desired performance levels?
9. How well are we prepared to meet the challenges of the present and future to deliver services to our clients and what do we need to do be prepared?

6. Developing Mission/Vision Statement

The mission statement of the firm would provide the context in which the goals and strategies are formulated, outlines the scope and direction, and provides the framework within which IT Strategic plan would be prepared. Specific technology projects and initiatives would be undertaken accordingly. For example, one of the goals regarding the use of IT in carrying out the firm's mission could be:

"We will use appropriate technology to provide effective tools for providing effective timely services to our clients."

To achieve this goal, we will:

- Encourage office-wide participation in identifying the right type of technology and tools required.
- Enhance the quality of services by appropriate use of technology to facilitate the sharing of information within the firm and with the clients as required.
- Provide opportunities for staff to research and develop new approaches and techniques to optimise the use of IT and provide necessary training.
- Develop and maintain an IT plan that encompasses the Technology infrastructure, IT process architecture, application software and relevant best practices for using IT in all key areas of services.

7. IT Strategy for SMPs Firms of the digital era

SMPs Firms must consider IT not merely as an office asset to be procured for use by their staff as an office automation tool, but as a critical infrastructure which has a strategic long-term impact on their service delivery capabilities. SMPs Firms, whether large or small, will be compelled to increase their IT budget as more statutory/ advisory services provided by Practitioners (CA,CS,CMA,etc.) will be offered through e-Governance. This will impact Practitioners (CA,CS,CMA,etc.) who are in practice or in employment.

Practitioners (CA,CS,CMA,etc.) in employment will have to develop an IT strategy personally in terms of knowledge and skill enhancement as required for career enhancement by identifying overall area of specialisation, aims and objectives.

As IT is an essential part of business planning and a key enabler for business success by many enterprises, IT strategy will enable SMPs Firms to identify relevant IT skill-sets and competency levels based on the needs of individual staff and firm. IT strategy has to include an appropriate plan of action for development, acquisition, and deployment of IT/IT capabilities, competencies and skill-sets in furtherance of agreed scope, area of practice, area of specialisation and career path for the staff. The process of providing service must consider IT as a key enabler to provide value addition to clients. The knowledge and skill enhancement must be based on the IT solutions to be deployed to provide existing/new services to clients.

For SMPs Firms, discussions with existing clients will help in understanding and identifying their expectations from the perspective of services rendered and required now and in the future. This is extremely important in determining the future course of practice. This may also reveal ways in which service to clients may be enhanced through the use of IT.

The most difficult thing to predict about IT is change and the pace of change. Overall, IT strategy by Practitioners (CA,CS,CMA,etc.) must take into consideration not only the current technology but also the emerging technology, so that they can perform and provide services to their clients effectively. Hence, IT strategy must be sufficiently flexible to be able to adapt to changing technology/client requirements and potential avenues of service.

8. IT Strategy Plan: Defining Roles and Deliverables

The objective of IT strategic plan is to continuously infuse technology to provide better and more efficient service to clients and improve internal processes. The commitment to use of IT

has to be key strategy in the firm's business plan. This is to be based not on technology for technology's sake but based on an overall understanding about how relevant technology can be used to improve staff efficiency and effectiveness in providing services to the clients.

The IT strategic plan must be in line with the overall strategic plan and ensure that IT is deployed for meeting business requirements to sustain and extend the business strategy. This requires that IT resources are managed and directed in tune with the business strategy and priorities while being transparent about benefits, costs and risks. A well-developed IT strategic plan improves key stakeholders' understanding of IT opportunities and limitations, requires assessment of current performance, identifies current IT capabilities, capacity, and human resource requirements, and clarifies the level of investment required in IT.

The IT strategic planning must be a standard practice and needs to be managed at principal/partner level. The IT strategy must be linked with the overall strategy of the firm and encompass all key service offerings and designed to build new business and value-added capabilities by leveraging the effective use of IT as required. IT strategic planning must be documented and regularly updated as per the overall goals of the firm.

9. Developing an IT Plan: Key Considerations

An IT plan should be developed based on IT strategy and should provide a clear perspective of the road ahead in terms of where the firm is headed in near future, area of specialisation, emerging avenues of practice, prospective clients and their needs. An IT plan should also consider the aspirations and objectives of SMPs Firms and take into account external factors such as potential avenues for growth and prospective clients, envisaged expected competition in the traditional areas, and regulatory requirements that will impact and influence development of career\practice.

In developing an IT plan, every key area of practice needs to be examined with a view to determining the extent to which technology may be used to enhance that aspect of the practice or to reduce its cost. Brainstorming sessions internally and those with external consultants can be useful for identifying ideas and exploring potential solutions. It is important to research, identify and use best practices and solutions, which will ensure that Practitioners (CA,CS,CMA,etc.)' own understanding and use of technology is maintaining appropriate pace with that of employer/clients in terms of knowledge, competencies and skills though not necessarily in acquisition of hardware and software. IT planning by Practitioners (CA,CS,CMA,etc.) must be an integral part of their career or of their firms' progress.

IT strategy and IT plan, if well-researched and implemented effectively, will enable Practitioners (CA,CS,CMA,etc.) to build up on their latent competencies and skill-sets, and to establish them as thought-leaders and strategic partners and, thus, remain increasingly relevant for the foreseeable future.

The most critical factor in developing an IT strategy plan is development of an IT plan. The IT plan should be derived from the IT strategy which in turn is based on the firm's overall strategy. The IT plan should provide a clear perspective of the road ahead in terms of where the firm is headed in the near future, the areas of specialisation, the emerging avenues of practice and services sought to be delivered to existing and prospective clients.

The IT plan should also consider the aspirations and objectives of the SMPs Firms and take into account the external factors such as potential avenues for growth, growth of existing clients, acquisition of new clients, envisaged expected competition in the traditional areas, and

regulatory requirements that will impact and influence development of practice. In developing the IT plan, it is critical to consider and document the technology architecture and application architecture of the firm and also of the clients.

In developing IT plan, it is important to understand that the Technology architecture refers to hardware, software, systems, methods, and standards that an organisation uses to develop and operate computer systems. It includes computer and telecommunications equipment, operating systems software, communications software, office automation/support systems, methods for developing and maintaining systems, and the organisation's assurance/compliance/consultancy policies, procedures and standards.

The key to developing services is the software applications used. Hence, it important to ensure that the application architecture encompasses the automated processes or systems that an organisation uses to support its programs for providing services to its clients. The application architecture also includes the interrelationship among applications in terms of sharing data, access to applications, and the presentation of applications to users.

10. Identifying Areas of Automation for SMPs Firms

IT has become all pervasive and is a key enabler in enterprises of all sizes and this is so even in enterprises providing services. SMPs Firms are impacted by IT in multiple ways:

1. By automation of client's operations resulting in most of the client's data turning digital.
2. Automated regulatory compliances can be performed digitally. Most of the compliances can be performed only by using automation.
3. SMPs Firms are compelled to use IT in their own offices as relevant to provide services of assurance, compliance or consulting.
4. Exchange of communication and Information has become extensively digital and paperless requiring technology by most of the employees in a SMPs Firms.

Thus, IT by default rather than by design has become critically relevant for SMPs Firms. Technology deployment by de- sign from a strategic perspective by SMPs Firms could act as catalyst of growth and key differentiator to not only provide current service offerings to existing clients but also develop innovative delivery capabilities for new service offerings to existing /new clients. This can empower SMPs Firms to stay ahead of the curve by enhancing capabilities and transform the way services are provided.

11. Typical areas of Services of SMPs Firms

The type of services provided by SMPs Firms varies based on overall mission, goal, primary focus, specific area of specialisation, size, clientele and specific competencies and skillsets. However, the typical services could be broadly classified as:

1. **Process Outsourcing**: This covers general services such as Book-keeping, Accounts Reconciliation, payroll processing, etc.
2. **Regulatory Compliances**: This covers tax payment, returns filing and other statutory requirements.
3. **Audit & Assurance**: This covers the various types of audits. Examples: Internal Audit, Tax Audit, GST Audit, Company Audit, etc.

4. **Consulting & Advisory**: This covers consulting and subject-matter advisory services provided. Examples: Financial advisory, management consulting services, etc.
5. **Litigation & Assessment**: This covers litigation & assessment services provided. Examples: Filing of Appeals, etc.

In the later chapters, specific list of IT solutions which can be deployed for automating each of the above areas are outlined to serve as a roadmap for implementation.

12. Strategy for providing services

Based on overall business strategy, the SMPs Firms may decide to focus on specific areas of services. In Practitioners (CA,CS,CMA,etc.)e of areas of specialisation identified for their future potential, it is necessary to consider in detail the current starting point - existing clients, staff, systems and supporting infrastructure - and to identify the gaps between the current situation and the future needs. Depending on individual circumstances the solutions may involve a drastic change, resulting in replacement of all key systems in a relatively short time scale. In the most of Practitioners (CA,CS,CMA,etc.)es, however, a more evolutionary approach will be more appropriate involving replacement and modification of existing systems within a less challenging time scale.

13. Developing IT infrastructure for delivering services

In planning for transition to future to IT has to be used as a key enabler, it is critical to consider the following key factors:

A. a) IT Skills and Competencies

An analysis should be made of the current level of IT Skills at both the management and staff level. An inventory of current IT resources of the firm and IT environment of all the major clients has to be made to arrive at the typical IT infrastructure and required skill sets. The policies, procedures, and practices of the firm in various areas of operation need to be evaluated against requirements of client and future direction of the firm's services. The challenge will be to identify the required IT Resources and relevant competencies. The skills needed for the future development of the practice of the firm using IT. IT strategic planning has to be in line with the firm's long-term goals and the future strategic requirements. Critical decisions have to be taken on staffing levels, responsibilities and skill requirements.

B. b) Applications and Data

The existing mechanism of delivering services and related procedures need to be evaluated from the perspective of automation. The types of software applications used and processes in the firm have to be reassessed to confirm whether they are in tune with the future IT strategy. Duplication of jobs needs to be identified so that they could be automated. Care must be taken to develop an integrated timetable for change which takes into account the abilities of staff, IT resources available, IT resources required and practices of the firm. A change management process has to be implemented mapped keeping in mind the overall objective of providing best services at optimal cost.

C. c) Technology Infrastructure

Based on the requirement assessment of IT of the firm, it is essential to identify areas of development of IT for ensuring appropriate IT solutions for the future. IT resource planning and related budgets need to be carefully assessed considering the rapid technological changes and importance of serving both the present and future clients. The required

infrastructure solutions need to be put in place and the staff trained to ensure that services offered meet the client requirements.

D. d) Delivery of IT Services

The way the firm provides services to clients, internal processes adapted and the means of delivery of such services has to be assessed and new methodologies and means of delivery of services must be developed in tune with the capabilities of implemented IT. A thorough review of the practices needs to be undertaken to update them in tune with the IT deployment of the firm. It has to be ensured that IT solutions implemented are in tune with the overall IT strategy and goals of the firm.

E. e) User Culture and Training

Developing and implementing identified IT Solutions and services is not just about acquiring the right technology but more about training people in required processes. At all stages in the process it will be necessary to consult as appropriate and to be aware of the extent to which managers and staff are themselves going to have to adapt in order to ensure the success of the implemented strategy. Issues concerning culture, working practices, policies and procedures, documentation and training needs must be an integral part of the IT planning process. The overall aim in reviewing each of these areas is to identify the gap between the current knowledge and skill levels based on present environment and that which has been identified as best suited for the firm serving its future needs in the most cost effective way.

Automation without having underlying processes and systems does not deliver results. Hence, it is important to focus on developing and updating processes and systems and standardising and then automating these processes and systems becomes easier and delivers results.

14. Approach to developing Strategic Plan

It must be clear by now that IT is best implemented using a strategic approach to achieve long-term success. A simple approach for developing a strategic plan/IT plan is given below:

1. **Allocate time for planning sessions as required**.
   Make appointments for your project with the team-members and stick to it. Please involve your key staff and take inputs from them. It may be useful if you treat your firm as an important client so that you remain objective and provide the right priority.

2. **Make a list of existing clients, services offered**
   This list should include staff strength, infrastructure specifically technology infrastructure, revenue streams, growth trends, key issues and challenges. Perform a SWOT analysis of strengths, weaknesses, opportunities and threats of your firm based on your current status. This is an excellent way to get a quick assessment of where your firm stands. Some of the key questions to be answered by you and your core team for key areas are given below.

   This list is only illustrative and not exhaustive but this can be a good starting point.

   a. **Start by listing your strengths.**
      i. Are you making the most of them?
      ii. Are you able to devote most of your time to develop your best clients or most profitable services?

   b. **Identify your firm's strengths and weaknesses**.

i. Do you have the personnel that you need to do all the work available you?
ii. Do you and your staff have the expertise to keep up with clients' changing needs, emerging regulatory requirements and new avenues in IT areas?
iii. Are you aware of the technology deployed by each of your clients?
iv. How does the technology deployment impact the services provided by you?
v. What is the current level of automation in your firm?
vi. How well are you using automation to deliver services?
vii. Do you have competency to provide services on IT implementation for your clients?

c. **Review existing and emerging opportunities**:
i. What are the opportunities and Where are they available?
ii. Do you have a plan to utilise these opportunities?
iii. Do you scan the environment by reading relevant articles/surveys/ regulations and websites?
iv. How well-equipped is your firm with required IT Infrastructure and skills to provide these services in these areas?
v. Are there new avenues for IT-enabled services which can be provided to your existing clients based on your current competencies?

d. **Review both external and internal threats.**
i. What is the obvious threat of competition from other firms?
ii. What are the risks of internal threats?
For example, does the bulk of your income come from one client or one type of client?
iii. Are you depending on few personnel for providing services?
iv. What are your/your personnel current competencies and skillsets in IT and related areas in view of emerging e-governance, e-filing and e-services?
v. Will you current service offerings remain relevant in the near future for your existing and new clients?
vi. Do you have the appropriate technology infrastructure to provide services?

3. **Based on SWOT analysis, list out all key findings and prioritise them**
i. Prioritise the list in order of importance and impact
ii. Segregate them in terms of impact on your business in short term and long term. Use IT related items for designing IT strategic plan.

4. **Create a vision for the future**.
i. Where do you see yourself/ your firm in three years in terms of service offerings, clients and revenue?
ii. Based on this, prepare a plan for the future. Your SWOT analysis could be a good indicator on how you can maximise your strengths and opportunities, minimise weaknesses and address threats.
iii. Use your priority list to prepare a master list of tasks/activities which help you to build roadmap for moving to the future. Itemise list in terms of competencies, infrastructure, technology, resources, etc.
iv. Use the IT related items as input for preparing your IT strategic plan for building the required competencies and skillsets and
v. Invest in technology infrastructure to automate the current service offerings and identified IT-enabled services.

5. **Implement the plan**

i. Implement the plan grouped into easily identifiable projects with individual deliverables, timelines, budgets, resources, monitor the progress and take correct measures as required.
ii. Establish personal accountability for each of the projects.
iii. Consider yourself as project manager tasked with implementing the project.
iv. Strategic planning is not a once a-year planning exercise. It is important to take action as per plan and monitor progress on a regular basis.
v. Build the required competencies by acquiring skills in appropriate technologies through hands-on and online training courses.
vi. Consult with peers in the area and use their expertise as required.

15. Standardise Processes/Systems with life cycle approach

For successful implementation of IT, it is important to spend time on designing systems and processes covering typical life cycle for delivering services.

Typical life cycle of process for delivering services by SMPs Firms could be outlined as:

1. **Organise**: Organise the resources as per required organisation structure with reporting responsibilities, job description, access rights, list of staff, services, IT and other resources required.
2. **Plan**: Plan for availability of these processes, systems and resources in a timely manner.
3. **Execute**: Implement the plan with required documented processes for performing services.
4. **Review/Report**: Monitor the delivery of services from planning to deliverable stage.
5. **Analyse**: Analyse the performance of the services and staff to ensure resource optimisation, timely delivery and achieving timely delivery of services.

The firm should review the list of services offered, documentation available to support these services and wherever required, develop standard documentation for all the key phases covering all the steps of delivering services from initiation to final deliverable. There are many tools available which can help in standardisation of the processes, but each firm has to work on what is their unique strategy of work execution that best suits their firm. If there is a structured process with specific steps, it becomes easy to automate these and train the staff so that standardisation in delivering of service is achieved.

16. Summary

The most critical aspect in developing IT strategic plan in a SMPs Firms is to review the current technology and application infrastructure in terms of future requirements and implement a migration plan by adopting the right strategies. This will require developing the future IT Vision that would deliver needed services to clients. The IT strategy plan must support and align projects with the overall Business Plan and the Strategy of the firm.

Developing IT strategic plan requires investment of time at partner/ principal level and involvement of all key staff and identifying areas of specialisation. Successful implementation of IT Strategic plan will empower SMPs Firms with the required enabling IT infrastructure, systems and processes to scale up and grow as per the vision and strategy.

The end result of IT strategy plan is clarity on what the firm stands for and what it wishes to deliver to its clients. Time has to be spent with multiple brainstorming sessions at various levels as this involves redesigning and re-envisioning the future of the firm. Once done, the IT strategy plan becomes the foundation for planning and implementing the right IT infrastructure with related solutions which will deliver as per expectations and standards.

The next chapter will use the guidance from the DCMM model and walk-through as to how to do benchmarking of the current status of IT deployment and plan implementation of planned IT infrastructure for the firm.

II. Designing Strategic Roadmap for implementing IT using DCMM 2.0 Model

17. Brief introduction to DCMM 2.0

We are living in an era of digital disruption, where everything around us is getting significantly impacted. From the products we buy to services we receive; newer models and newer delivery channels are the order of the day. This dramatic change is impacting not just larger institutions, but also significantly impacting the way every establishment operates. This makes it imperative for any business to adopt technology and render better services and products. As Chartered Accountants, we need to adopt this digital wave and render services harnessing the power of technology to be relevant. This is often referred to as the 4th Industrial Revolution or Industry 4.0. Emerging technologies such as data analytics, blockchain, artificial intelligence, and machine learning, have the potential to be the real game changer for the profession.

The post COVID-19 era is an era of Digital epiphany. It is an era of automation, an era of investing into technology and era where technology enabled solutions would be the order of the day. This makes it imperative to invest in technology. At the same time, one should realise the importance in using technology in the workplace and improving the efficiencies. One should realise that technology is an enabler for us to perform better and automate the mundane tasks which at the same time can enhance the productivity.

Digitalization and technology have impacted the way our profession is perceived. These trends not just demand a change in thought process but also a fundamental shift in the way professional accounting firms are run. As newer digital technologies continue to emerge, accounting firms must anticipate and gear up for the technological revolution. Digital Accounting and Assurance Board (DAAB) of The Institute of Charted Accountants of India (ICAI) has taken up an initiative to assess the digital competency of professional accounting firms and to guide them on how they could scale up and ride the tide of technology.

In the previous section, we have learnt how to prepare a IT strategic roadmap and this must have resulted in identifying specific IT initiatives to be implemented in specific areas of services. It would also have identified project teams to be vested responsibility for ensuring deliverables from each of this IT initiatives. In this section, we will understand how to use DCMM model to benchmark what is the current status of IT implementation and identify areas to implement and prioritise them in order of priority.

While SMPs have slowly started realising the power of technology, they are also faced with a challenged as to how to get started with the technology journey. This is where a structured approach is necessary. Digital Competency Maturity Model For Professional Accounting Firms - Version 2.0 And Implementation Guide (DCMM 2.0) by The Institute of Chartered Accountants of India (ICAI) through Digital Accounting and Assurance Board (DAAB), has initiated a process of laying out self- evaluation matrices for accounting firms to gauge their relative maturity level as regards digital competency.

This newer version has taken into account the discipline specific categorization of accounting firms and related technology adoption for achieving efficiency and productivity gains. It also includes a new section on emerging technologies and also provides guidance on implementation of each of the sections.

2. Overview of the DCMM 2.0

DCMM Version 2.0 comprises a questionnaire that enables firms to rate their current level of maturity on digital competency, identify areas where competencies are strong or lacking, and then develop a road map for achieving a higher level of maturity.

DCMM Version 2.0 includes the following dimensions of digital maturity organized into sections:

- **Section A: Level of Automation of Firm's Internal Processes:**
    - This Section covers extent of usage of IT by the firm for its own internal processes for example, billing, document management, client relationship management, and staff attendance and work tracking, cyber security, compliance with data protection regulation and social media presence.

- **Section B: Availability of Qualified Resource Pool and Talent Development Relating to Digital Competencies:**
    - This Section covers aspects like, attracting, retaining and developing staff with requisite qualifications and skills.
- **Section C1 (Discipline specific Categorisation – Audit):**
    - Level of Automation Relating to Audit Processes and Nature of Audit Services being Rendered –
        - This Section covers the level of automation at client's end, access to automated audit tools, training of employees on audit tools, ability to handle digital evidence, Information Technology Audits, etc.

- **Section C2 (Discipline specific Categorisation – Tax and Compliances): Level of Automation Relating To Tax & Compliance Processes And Nature Of Tax and Compliance Services Being Rendered**:
    - This Section covers the level of automation at client's end, access to automated tax and compliance tools, customisation of tax and compliance tools, training of employees on such specific tools, etc.

- **Section C3 (Discipline specific Categorisation – Accounting and support function): Level of Automation Relating to Accounting Processes and Nature of Accounting Services being Rendered**:
    - This Section covers the level of automation at client's end, access to automated accounting tools, training of employees on client accounting tools, etc.

- **Section C4 (Discipline specific Categorisation – Other Management Consulting Services): Level of Automation Relating to Other Management Consulting Services being Rendered**:
    - This Section covers the level of automation at client's end, access to automated miscellaneous tools, training of employees on tools, management consultancy services, forecasts, M&A Advisory, consultancy services, training activities, etc.

- **Section D: Adaptation of Advanced and Emerging Technologies:**
    - This Section covers the extent of adaptation of advanced and emerging technologies like, Advanced Excel, Use of Data Analytics, Adoption of Robotic Process Automation, Artificial Intelligence, Social Media, etc.

In CA Firm is engaged in more than one type of service then applicability of Section C1, C2, C3 and C4 should be checked individually. Further, if more than one discipline specific categorisation is applicable, then firm should fill all the applicable Sections. In Case a particular section (C1, C2, C3 or C4) is not applicable to them, the firm can ignore the same and proceed with the subsequent Section.

3. Firm Maturity Rating

Scores obtained in each of the respective Sections should be interpreted independently to determine firm's maturity with respect to that particular Section. The rating categorises the firms under the following 3 Levels:

- **Level 1 Firm:** indicates that the firm is in very nascent stages of adopting digital technologies but will have to take immediate steps to upgrade its digital competency or will be left lagging behind.
- **Level 2 Firm:** indicates that the firm has made some progress in terms of adopting digital technologies but will have to fine tune further to reach the highest level of digital competency.
- **Level 3 Firm:** indicates firms which have made significant adoption of digital technologies and should focus on optimising it further to be in the forefront of use of emerging technologies like, Artificial Intelligence and Blockchain.

4. Implementation Guide

Competency dimensions mentioned in each Sections are targeted to enable firms to assess their current digital competency for moving to the next level. In order to assist professional accounting firms to achieve various competency dimensions, DCMM Version 2.0 includes implementation guide in the form of implementation clues. These clues are practical based and are a sort of handholding for small and medium firms for adopting new technologies.

The Implementation Clues given in this guide are generic and are minimum requirements under each domain. The firm is, however, free to adopt better practices. Further, names of some websites have been included as an example to help the firms in adopting new technologies. These examples are only illustrative in nature and is not meant for

promoting/ recommending any particular website, and the list is based on market research conducted by the authors while drafting the clues.

This Implementation Guide is prepared to assist the Professional Accounting Firms (Firms) in implementation of the various digital initiatives and enhances their digital maturity competency. Please refer to the DCMM 2.0 model and implementation guide for more details. This can be downloaded from: https://resource.cdn.icai.org/57964daaab47265.pdf

Prior to using this guide, the accounting firm should have assessed their existing digital competency maturity using the evaluation questionnaire available at ICAI website https://learning.icai.org/committee/irg/digital_insights/digital_competency_maturity_model_version_2.0/

5. Benchmarking current status using DCMM 2.0 Model

The below mentioned steps can help you benchmark and assess the current status using DCMM 2.0 Model:

Step 1: Benchmarking

Benchmark the current maturity level of the firm by completing the DCMM, and document list of specific aspects that the Firm is currently lacking, and which needs to be initiated to move the next level of Maturity model.

Step 2: Planning Initiatives

Convert the initiative to be taken into an action plan- with timelines- quarterly/annual.

Step 3: Identifying resources and execution plan

Identify a small cross functional team to own the execution of the plan, with a leader and make the execution of the plan, an important part of the Key Result Areas/KPI of this team. Define accountability for reporting progress and challenges in implementation.

Step 4: Assessing progress and re-validation against the DCMM

Assess the progress by re-evaluating against the DCMM and re-visit the execution plan half-yearly.

Step 5: Perform a peer review/ review by external firm, if necessary

The firm may on a voluntary basis perform a review by an external firm or a peer review and assess the position at periodical intervals. It is recommended to perform peer review on a regular basis by external firms or at the time when firm ascends to next level.

6. Using findings from Benchmarking to identify areas of implementation/improvement of IT deployment

On successfully assessing the Firm's Maturity with respect to the various Sections in DCMM, one should identify the areas for improvisation, automation. The Implementation Guide of DCMM (available at https://www.icai.org/new_post.html?post_id=16231) could be a handy guide to benchmark. The below steps could be a good way to get started after assessing the digital maturity of your firm using DCMM 2.0.

1. Identify the results from the DCMM 2.0 and identify areas for improvisation / automation / process improvement.
2. Refer the Implementation guide on each sub-section of the specific Section of DCMM 2.0
3. Identify the required **tools, processes, and skills** for the reaching the next level of maturity
4. Form a committee / identify a responsible stakeholder in the leadership to bring this change. It is important that the senior partner / proprietor is personally involved to bring the transformation
5. Acquaint, explore and understand the various tools available in the market. One could refer the subsequent section on the list of tools available.
6. Upskill the firm with the required skill set. e-Learning, Online training, self-paced training models can be considered.
7. Define the new processes within the firm. Develop Standard operating procedures (SOP) and enable the firm to be a process driven from people driven.
8. Run a Proof-of-Concept (POC) / test an internal use Practitioners (CA,CS,CMA,etc.)e using the tools identified.
9. Learn from issues identified and success of the proof of concept. On the successful completion, implement newer measures and scale it up across all employees / departments.
10. Continuously repeat these steps for each of the gaps identified to mature. Reassess once in 6 months or once in a year.

7. Prioritising IT deployment based on cost-benefit analysis and growth strategy

Prioritising the right IT deployment based on the strategy of the firm is a very essential requirement. Considering the time and resources are in short supply yet high demand, prioritizing IT deployment becomes all the more difficult. Evaluating and prioritizing projects can be complex, but this vital first step can negatively impact if not assessed carefully. The below listed are a few steps:

1. **Prioritise projects based on value to the Firm**

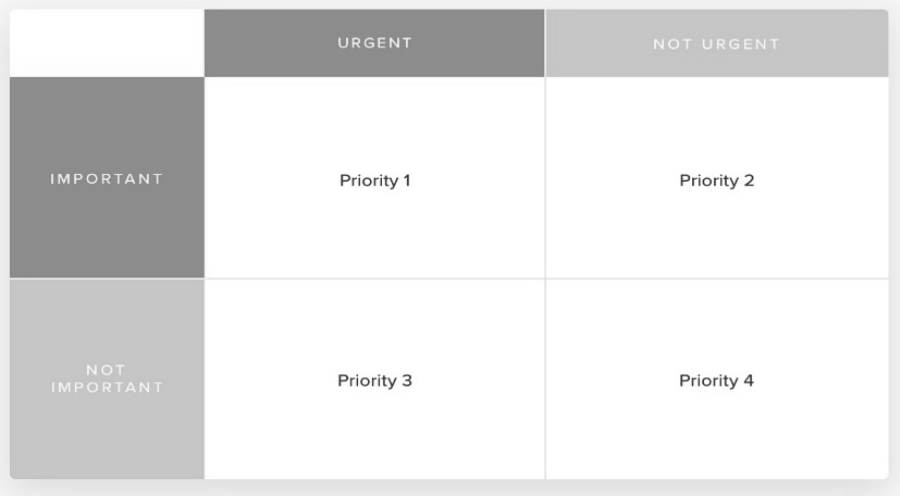
   One could begin by looking at each project on the list and ask a simple question: “How will this project / IT deployment impact my firm?” Projects which can bring in more clients, improve efficiency, render better quality of services, should take the priority.

2. **Set priorities by identifying urgent and important projects**

   With COVID-19 and remote working, solutions pertaining to remote working may be a priority in comparison to developing a website. Choosing the right prioritization matrix is essential process. While the IT deployment may be important, it may not be urgent.

   - An important project brings value to your business, whether you feel its impact today or years down the road.
   - An urgent project requires immediate attention to stay on track or keep business going.

One could consider deploying the time management matrix by Stephen Covey which could make it easy to prioritize work into 4 simple buckets.



Urgent vs. Important Priority Matrix

Priority 1- Urgent and important: These are a hard deadline that one can't afford to miss? These must be prioritised first. Ex: Deploying a work from home technology, IT Security Solution etc.

Priority 2 - Not urgent but important: These are important projects, but do not have an immediate deadline but matter to the firm. Ex: Implementation of Task Tracking Tool, Deploying Data Analytics for improving quality of engagements etc

Priority 3—Urgent but not important: These projects may call for quick attention but may not serve the goals of the firm. There is a possibility of delegating it. Ex: Deploying an IT Solution which may be a required for only one client engagement or for an one-off engagement.

Priority 4—Not urgent and not important: These projects can be ignored for the time being, so that once can free up some time and resources for more worthy work. Ex: Introducing an Asset / license tracking tool/preparing a solution for internal training, knowledge repository etc.

3. Assess the firm's bandwidth

The priority should be also decided based on firm's bandwidth and available resources including time and money. While technology should not be considered as a cost and rather as an investment, it is important to strike balance with the investment versus the benefits which the firm would obtain. Equally important is the availability of time for the key members of the implementation team / committee, as they would have to balance their existing projects in hand and also look into the technology deployment.

This table could help firms in doing an overall comparison from the various options:

#	Gap Identified	Firm Priority in fixing	IT resources required	Vendors and product pricing	Time involved in deployment, training
1					
2					
3					

There is a need for SMPs Firms to change, and even more important is the fact technology is forcing us to! As practitioners, starting from simple tools to keep track of daily tasks to advanced analytics tools which can give valuable insights, there are various methods in which

technology can be adopted at our workplace. In this Journey of Digital Transformation, we must focus broadly on the following:

Mindset

- Develop a strategy
- Who do we want to be, what services do we want to deliver to clients?
- How do we build the business model around this?

Skillset

- What skills do our staff need
- How do we make sure they obtain these?
- How can we attract people with the right skills?

Toolset

- What tools can we use to leverage our strategy?

8. Using DCMM implementation strategy to prepare roadmap with milestones and deliverables

F. Case Study – SMPs Firms & Co.

M/s ABC & Co, a SMPs Firms, after doing a self-evaluation using the DCMM checklist, has identified that in the following areas, the firm is lacking in adoption of Technology or structured process:

Section – A - Level of Automation of the Firm's Internal Processes

1. Non-availability of Corporate email IDs for their Staff
2. No social Media presence
3. No Structured leave management system
4. No tagging of employee assets
5. No Centralised server management system
6. No CRM / HRM workflow tools
7. No Time Sheet system in place
8. No structured / automated backup system in place
9. No Mobile Device Management (MDM) Policy is in place
10. No IT Policy

Section – C1 (Discipline specific Categorisation – Audit)

1. IT Controls are not reviewed before the start of the audit.
2. No tool used for audit planning, scheduling, resource deployment, tracking hrs/days spent vs. budgeted time, etc.
3. No automated tools being used during audit.
4. The audit staff have limited understanding of the end to end automated processes of the client.
5. No CAAT tools / Data Analytics tools being used.

The firm can now prioritise, their activities from the above gaps identified, based on their requirement. The below could be a simple justification summary:

Section - A

#	Requirement	Firm Requirement	Priority
1.	Non-availability of Corporate email IDs for their Staff	Required as this client's data is confidential and personal email should not be used.	Medium
2.	No social Media presence	May not be a required at the current situation	NIL
3.	No Structured leave management system	Necessary to track article / employee leave and tasks done.	Low
4.	No tagging of employee assets	May not be a required at the current situation	NIL
5.	No Centralised server management system	High priority to safeguard the data	High
6.	No CRM / HRM workflow tools	May not be a required at the current situation	NIL
7.	No Time Sheet system in place	Necessary to track article / employee leave and tasks done.	Low
8.	No structured / automated backup system in place	High priority to safeguard the data	High
9.	No Mobile Device Management (MDM) Policy is in place	May not be a required at the current situation	NIL
10	No IT Policy	May not be a required at the current situation	NIL

Section – C1

#	Requirement	Firm Requirement	Priority
1.	IT Controls are not reviewed before the start of the audit.	Majority of the clientele of the firm operate with limited IT Environment such as POS Machines and Accounting Tools such as Tally. Reviewing the critical IT controls of such applications may not be a requirement for the firm now.	NIL
2.	No tool used for audit planning, scheduling, resource deployment, tracking hrs/days spent vs. budgeted time, etc.	The process of audit is not standardised and reliance on work papers will have to be improvised. The firm is considering deploying tool to standardise the audit process including risk assessment, resource deployment, managing time sheets etc.	High
3.	No automated tools being used during audit.	To increase efficiencies and to automate repeated processes, the firm is considering using deployment of tools	Low
4.	The audit staff have limited understanding of the end to end automated processes of the client.	Majority of the clientele of the firm operate with limited IT Environment such as POS Machines and Accounting Tools such as Tally. Reviewing the critical IT controls of such applications may not be a requirement for the firm now.	NIL

5.	No CAAT tools / Data Analytics tools being used.	CAAT Tools assist in automating audit process which manual and repetitive in nature. Considering all clients deal with digital data, these tools are handy to perform analysis.	Medium

On identifying the priority items, the SMPs Firms takes next steps to evaluate the various solutions:

#	Gap Identified	Firm Priority in fixing	IT resources required	Vendors and product pricing	Time / Steps involved in deployment, training etc.
1	No Centralised server management system	High	Centralised Server and with all the data stored. Depending upon the type and the quantity of data involved either a "Server Computer" such as Windows Server may be deployed. Alternatively, a Personal Computer, with high end configuration such as 1 TB Hard disk Storage, 4GB RAM etc may be chosen	**Vendor A –** Price – INR 38,000/- + GST No Free support **Vendor B –** Price – INR 40,000 + GST 1-year warranty and support	1. Identify the type of Solution to be deployed. 2. Finalise the budget 3. Deploy the hardware and software 4. Migrate the data from the existing systems to the new systems 5. Test check if the migration is successful 6. Retain the old copy of the data for future reference.
2	No structured / automated backup system in place	High	Cloud based back solution OR Real-time synchronisation with Google Drive / Microsoft OneDrive / Zoho Work drive OR	**Vendor A –** Cloud based back up scheduled once in the day INR 25,000 per year **Vendor B –** Microsoft One Drive 1 TB – INR 330 per month onwards **Vendor C –**	7. Deploy the identified solution 8. Install the software if required 9. Deploy the client console for taking the backup

AJA #NEWTHINKING

#	Gap Identified	Firm Priority in fixing	IT resources required	Vendors and product pricing	Time / Steps involved in deployment, training etc.
			Periodically backing up through External Hard Disk	1 TB Hard Disk INR 3,500 onwards	10. Define a process to take backup / verify the backup 11. Check regularly for restoration.
3	No tool used for audit planning, scheduling, resource deployment, tracking hrs/days spent vs. budgeted time, etc.	High	Software which have the following capability: - Creating tasks, sub tasks and checklist - Assigning and uploading documents against each of them - File archival system - Time Sheet tracking and approval.	**Vendor A** Cloud based Audit Management Tool INR 250 per user per month **Vendor B** On premise office management system INR 10,000 onwards Vendor C Cloud based office management system INR 300 per user per month.	12. Assess the utilities in each software. 13. Confirm how the data is being stored and kept confidential. 14. Identify how the support and backup would be taken care. 15. Explore if the tool can assist in office management in addition to audit tracking.

9. Developing standard checklist for evaluation of specific IT solutions as required

G. For Hardware Deployment

The choice of right hardware determines the subsequent steps in deploying any technology. The traditional model of computing is the Client-Server Model which is a is a distributed application structure that partitions tasks or workloads between the providers of a resource or service, called servers, and service requesters, called clients. Under this method there is a locally hosted server, which could be a designated server for emails, for storage, for files, as a database, for a specific application such as Tally, etc.

Under this Technology the firm will have to invest in the infrastructure, networking resources, database and the application. In addition to this, the firm will have to assess the maintenance cost such as periodical / regular updates, backing up of the system etc.

It is to be noted that while deploying the required hardware, the general thought process would be to keep a High End system for the partners, and commonly accessed Servers and keep a

machine with limited configuration with the other end users. This will ensure the cost is kept at minimal while trying to achieve the optimal efficiency.

The following should be considered while deployment of Hardware:

1. **RAM**
   The higher the RAM, the faster is the processing capability. It is recommended to have atleast 4GB of RAM and above, even though 2GB RAM does the basic work. In case of advanced computations, dealing with large data sets, it is suggested to have a RAM of 12GB and above. Enhancement of RAM is possible for existing PCs / Laptops subject

2. **Hard Disk Space & Type**
   a. **Types of Hard Disk**
      i. HDD Servers are the traditional mechanism of a storage device that uses mechanical platters and a moving read/write head to access data. Since all pieces are “mechanical,” the hard disk is the slow.
      ii. SSD servers are configured with the Solid-State Drives that guarantee top of the line performance. A super-fast hosting for high performance is possible on SSD storage which works much faster than normal HDD server.
   b. **Space of Hard Disk**
      The minimum range of hard disk space today starts from 128 GB, even though 512 GB and 1TB are the most popular. For an average CA office of about 100 clients using tally, on premise tax software etc., a server / computer with a minimum storage of 512GB to 1 TB would be sufficient.

3. **Processor Speed**
   Computer processors and their clock speed are two features which are most commonly associate with high-performing, fast technology. The CPU is often referred to as “the brain” of the computer. Most computers also have multiple processor cores that enable computer to complete multiple tasks at once, say edits to a document, while watching a webinar. Processor speed is measured in gigahertz (GHz). The higher this measurement, the faster the processor.

For Software Deployment

It is important to appreciate that the right software can help any professional drive business improvement, grow their business, and better manage challenges. As a best practise, it is always recommended to test whether the software is meeting the current and future needs and compare it with competitor products every few years. While changing software can be challenging, one could end up with software that better helps you improvise the existing processes. With developments in technology, one should give preference to cloud-based (online) solutions over other options.

The following is a list of tips could help select the right software for your firm:

1. **Understand firm strategy:**

   The investment in software systems should not only meet the current needs but should also be adaptable to meet the future needs of the firm. It is therefore important to know where the firm is heading over the next 3 to 5 years.

2. **Linking processes**

It is important to link the business processes to functionality of the software. Process mapping will also assist to identify processes that should be automate or eliminated.

3. **Understand the model of deployment**
   Largely software vendors today have two models viz., on-premises (installed at your office computer / server / laptop) or over the Cloud (such as SaaS based solution) which can be accessible anywhere over the Internet. Care should be taken to evaluate the cost benefits of both before drawing conclusion. Refer subsequent section on comparison of cloud vs on-premise

4. **Using standard functionality**
   Customising software to match business processes and the functionality carries long-term risks, such as problems with maintaining, updating, and upgrading software, costs of supporting customised software and higher training costs. It is better to rely on standard functionality, which may mean reconfiguring processes to match the software rather than customising the software.

5. **Testing with real use Practitioners case**

   It is recommended to test the software choices using real data from your firm, over a reasonable period, before making the final decision. Consider whether it has the functionality desired and is it easy to use? Does it produce the required reports, and does it integrates with other software used by the firm.

6. **Cost benefit analysis**

   Identify all the costs of acquiring new software including on-costs and weigh those up against the benefits before making a decision. Cost should not be the sole factor in determining which system is best for your business.

7. **Training & Support**
   Information on the training and support available from software providers – upfront and on an ongoing basis – as well as costs involved for extra support

8. **Limitations of the Application**
   One should carefully assess the limitations of each application and take a call on which application to use and what are the features in built into the application.

9. **Data Migration**
   Identify the process to migrate the data from the old systems to the new system. This should be done carefully to consider the requirements and formats of the new software.

10. **Security and other Certifications of the Vendor**
    If the software is in the cloud, check the terms and conditions carefully to see the level of security
    offered, who owns the data in the cloud, where the data centres are physically located and the process for retrieving data if you leave that provider. Also consider the quality of your internet connections, paying attention to both download and upload speeds

11. **Due diligence on the software vendor**

Do some due diligence on the software provider as you want to avoid purchasing a package from a provider that becomes insolvent. Also creditability and long standing are factors one should consider.

H. Bring Your Own Device (BYOD Policy)

While the firm might deploy their own assets, many of the firms require the employee / trainee to bring in the laptop / notebook computer. Some other firms have a policy where the assets are over the period of training / employment transferred to the employee of the company. While BYOD brings in flexibility, it poses a few concerns from a Security angle.

The following are recommended best practises to follow with respect to BYOD.

a. Define a policy on what is permitted and not permitted with respect to BYOD Assets, licenses, and software. An example could be devices not to Store or transmit illicit materials, transmit proprietary information belonging to another company etc.
b. Deploy Endpoint Threat Detection and Response (EDR) and firewall solution. EDR not only includes antivirus, but it also contains many security tools like firewall, whitelisting tools, monitoring tools, etc. to provide comprehensive protection against digital threats.
c. While connecting over the office Wi-fi, it is recommended to deploy controls such as MAC ID based configuration, which ensures only select systems of the employee are connected to the network.
d. Consider regularly auditing / scanning the systems to identify policy violations
e. Sign required confidentiality agreements and obtain regular confirmation from employees on the confirmation of the same including educating employees on their liabilities in case of breach etc.

10. Developing standard deployment model for automation

While the firm intends to increasingly deploy automation into their services, it is critical to understand the deployment model for each of the potential automation. While there cannot be a one size fits all solution, the following are good indicators:

a. Identify the avenues for automation.
b. Identify the root cause of the problem and how best an automation solution can fix it.
c. Assess various options for automation from in house developed macros or tools to using external software solutions
d. Assess the cloud solutions which can automate various activities.
e. Test check the options and run a proof of concept.
f. Learn from issues identified and success of the proof of concept.
g. Train the users and upskill them.
h. Run a full-fledged implementation

11. Integrating Firm's processes and systems with IT solutions

Given below is an illustration on how one can integrate firms processes and systems with IT Solutions. Consider the firm intends to deploy "Data Analytics" for doing their audit engagement. The below steps could be followed:

Steps	Illustration / Tools required
1. Identify the Audit objective.	An example could be GST reconciliation, Identify Duplicate Payments, compare select transactions over two periods (say Payroll)
2. Obtain the data from the source file	Tally, Payroll software, GST website could give the required format.
3. Cleanse / Curate the data	This is required to bring in the data in the desired format so that one can proceed with analysis. Excel / Data Analytics Software can help cleanse and curate the data.
4. Profile the data	This is required to profile the data to obtain an overall understanding of the data. Column totals, statistics etc can be used here.
5. Analyse & Investigate	This involves various activities performed to conclude on the audit tests. Functions such as lookup, Compare, consolidate, pivot, identify duplicates and help perform the audit tests to meet the audit objective
6. Report the findings	The issues identified and the observations are documented and reported.

12. Summary

DCMM 2.0 is an excellent yardstick for a firm to mature digitally. Most SMPs Firms are compelled to use technology, but the extent and diversity of technology deployed varies significantly depending on the size, type of clientele, area of services and overall IT culture and awareness of the firm's senior management. Whatever be the extent of IT deployment, there is always scope for improvement and to take it to the next higher level.

There could be many possibilities of improvement. Some examples are:

- Scope of implementation could be increased.
- Newer areas of service could be covered.
- New technology could be deployed.
- Latest and higher level of automation could be deployed.
- Newer solutions could be implemented, etc.

DCMM model could be used by SMPs Firms regardless of level of technology deployment to identify current status of technology deployment, assess whether this is adequate to meet firm's goals, identify newer/higher levels of technology, areas for implementing, etc. DCMM could also be a starting point for any firm to begin climb upwards on their digital journey. This coupled with the implementation guide could enable the firm to start executing their digital initiatives in a strategic rather than ad hoc manner.

The need for SMPs Firms to operate virtually has been demonstrated during this covid times of uncertainty. Operating as a virtual office would mean that the firms' physical office could only be an address or meeting point whenever required and most of the work can be done from anywhere/anytime by using the digital infrastructure of the firm. The stakeholders of SMPs Firms must have a digital platform to access/exchange information online with each other and client for performing/delivering service as required regardless of their physical location.

This model of remote working/virtual office is increasing every day and it only makes business logic for SMPs Firms to gear up to implement this as quickly as possible. This requires a

fundamental shift in the mindset of the firms and adequate toolset which can help the firms mature in their digital journey. Care should be taken to understand the unique requirements of their firm and see how best one can solve it. While one size fits all approach cannot be followed, the attempt to become virtual firm should be targeted with specific timelines and deliverables.

The previous two sections of this book have provided a roadmap, guidelines, and tips to go digital and eventually virtual using a strategic and structured approach. This can enable SMPs Firms to operate virtually as per their needs using relevant technology solutions. The objective of this publication is not to provide specific solutions but overall approach at a macro level. There are other publications and many webinars of ICAI covering specific areas of IT implementation. It is important to know that Technology is available within reasonable and affordable budgets which will suit most firms. What is required is the mindset to implement and put in the time and effort for implementation. We hope you will begin your digital journey sooner than later! Time is of the essence in the current times more than ever!

The next chapter will focus on providing guidance and tips on how to identify and evaluate specific IT solutions as per overall strategy, vision and goals of the firm.

III. Identifying and evaluating specific IT solutions

1. Technology Solutions: an overview

Technology is changing the way we work and live. In this constantly evolving digital landscape, things do not seem slowing down anytime soon. Companies have to re-think how they do business with their customers, the skill sets of the people they employ, and the tools they have in place to maximise efficiencies and safeguard profit. The impact of this is not just in business but on our profession too. If we do not adopt to this digital wave, we have a risk of losing out to the competition or worse, risk of being taken over by machines!

Digitalization and technology have impacted the way our profession is perceived. These trends not just demand a change in thought process but also a fundamental shift in the way professional accounting firms are run. In preparing for the future, we must think about what tomorrow looks like, how they remain relevant, and how they position themselves and their firms for this change. As newer digital technologies continue to emerge, accounting firms must anticipate and gear up for the technological revolution.

It is therefore important for us to understand Technology and how it can impact our Profession. Small and medium-sized firms (SME Firms) are unlikely to have a dedicated IT Department or Help Desk, it still has to perform all the same tasks as a large organization and should ensure that those tasks are allocated to someone within the business or to an external service provider.

Effective selection, implementation, and management of technologies, as well as training employees to use software solutions, are fundamental to the success of any firm.

When introducing or reviewing a technology strategy, a firm needs to first define what it wants it to do. Then, find a system that will achieve them. Technology will assist a firm in, among other things, the following aspects:

- Efficient tracking and scheduling of work.
- Maintaining records and contact with the firm's client database
- Sharing data with their clients.
- Improvisation in the communications process
- Storing and retrieving data efficiently and with adequate disaster recovery mechanisms
- Enhancing the presentation of the firm's work
- The marketing of the firm and their value proposition; and
- Managing time pressures.

2. Some Tips on IT Automation for SMPs Firmss

As technology keeps evolving, there are newer and newer solutions covering hitherto uncovered areas, the SMPs Firms should always be on the lookout for what new solutions are available for automating their existing manual processes. However, the best approach is to consider what are the pain-points in providing service deliverables and ensuring quality and focus on automating them. Further, the firm can also consider areas of service which has the maximum revenue/value or impact and work on automating the service. In automation, it is not how much but how well it delivers value to the client.

One of the key points considered while evaluating IT solutions by SMPs Firms is how much does it cost and can we afford it now. Please remember that IT automation of SMPs Firms has to be considered from a strategic and long-term perspective and hence it has to be considered as an investment and not just an expense item.

IT automation done well can provide ROI quite quickly apart from brand-building, saving time and improving efficiency but most critical consideration is not just the investment of money but the investment of time to make the solutions work by training/adapting as required.

3. Core Technology applications in a SMPs Firms

The range of services provided by a SMPs Firms would vary depending on age, size, area of specialisation, its clientele and type of business they operate, core competencies of the firm, and vision of the firm. Hence, this would impact the type of automation required by the firm. Some examples of the core applications relevant to the effective use of technology in a SMPs Firms would typically include: (this list is illustrative and not exhaustive)

1. A practice management system which records firm's performance, including work in progress and status of tasks assigned
2. Time-recording software (generally, this comes with integrated billing modules for raising invoices as well as monitoring time and productivity by person and by client);
3. An invoicing software which is linked to the tasks performed and receivable management.
4. A book-keeping software capable which is regularly updated and capable and having templates which conform to statutory accounting requirements such as GST and Income Tax
5. A diary or personal organizer software where multiple people have access to a single diary.
6. File-management and archival system.
7. Client relationship management (CRM) software.
8. Word-processing, spreadsheet and presentation capability software
9. A database system capable of creating your own personalized applications (optional);
10. An Internet connection with a redundant connection as a fall-back option
11. A web site for your firm and a domain email ID.
12. A fixed asset and software license tracking system
13. An accounting and compliance automation tool which would enable faster data entry, meet the regulatory requirements etc.
14. Speciality applications to assist firms to automation of many procedural tasks.

4. Technology for SMPs Firms: An Overview

As we know that Information Technology continues to evolve rapidly with faster, more reliable, and cheaper Internet connections and fundamental changes in how applications are developed, deployed, implemented, and used across the world. Research indicates that investment in technology is a key driver in productivity in any enterprise and this is true for a

SMPs Firms. The partners/owners/staff of SMPs Firms are not expected to have technical expertise, but they need to have working knowledge of technology as relevant for SMPs Firms.

This section provides a brief overview of technology to make the team at SMPs Firms well-conversant with some of the fundamental aspects of technology:

a. Server Client based Technology

Client–server model is a distributed application structure that partitions tasks or workloads between the providers of a resource or service, called servers, and service requesters, called clients. It is the oldest and the traditional method of computing. Under this method there is a locally hosted server, which could be a designated server for emails, for storage, for files, as a database, for a specific application such as Tally, etc.

Under this Technology the firm will have to invest in the infrastructure, networking resources, database and the application. In addition to this, the firm will have to assess the maintenance cost such as periodical / regular updates, backing up of the system etc.

b. Cloud based Technology

Cloud Computing means the use of computing resources as a service through networks, like internet. It is the use of various services, such as software development platforms, servers, storage, and software, over the different networks, often referred to as the "cloud." Ex: Google apps.

Cloud computing facilitates anywhere/anytime access to real-time data. The benefits include improved efficiencies, increased availability, elastic scalability, fast deployment, and low upfront costs.

These models are usually charged on a pay per usage and per user basis. Cloud providers offer services using three models:

i. Software as a Service (SaaS)

- It provides ability to the end users to access an application over the Internet that is hosted and managed by the service provider. SaaS has a significant impact on how firms do business and interact with their clients by providing a cheaper and easier technology solution.
- Cloud-computing applications are hosted by a service provider and accessed by customers over the Internet, often with a simple web browser but sometimes with a small application automatically downloaded from the hosting provider.
- Instead of investing heavily on technology, the firms rely upon external service provider who has hosted the application over the internet and the firm may now work on the same sets of data online.
- The firm need not spend on buying the software but pays only for service as per the license agreement for the specified period.

ii. Platform as a Service (PaaS)

- PaaS is a cloud solution for the creation of applications. In this model software, developers have access to computing platforms including operating systems, programming language, and execution environments without the underlying infrastructure costs.

- This model is beneficial where the firm intends to build customised applications without incurring much cost, as the cost of servers, virtualisation, storage and networking is taken care by the service provider.

iii. Infrastructure as a Service (IaaS)

- IaaS is a cloud solution where the cloud service provides fundamental computing services such as a server, storage, and a network as an on-demand service.
- In this model the firm is responsible for maintaining the operating systems and applications software including platform for creation of applications.

Out of the above 3 models, SaaS model is highly preferred as the firm need not invest heavily in the infrastructure, maintenance, regular updates, network or servers and merely uses the software / application developed by the service provider over the internet. The firm focuses on optimising the client data to obtain the desired result such as financial statements, tax returns, valuation models etc.

Now the real big question is how to decide between an In-house versus Cloud based Application or when should the firm move to a cloud-based application?

Key Factor	On-Premise (Traditional Computing)	Cloud Computing
Deployment	✓ Resources are deployed in-house and within an enterprise's IT infrastructure. The firm will have to invest in the infrastructure in addition to maintaining it.	✓ Resources are hosted on the premises of the service provider, but the firm would be able to access those resources over the Internet. The firm need not invest in hardware, infrastructure or regular maintenance of the same.
Cost	✓ Since the resources are deployed in-house, the cost of servers, networking, application would be high. Alternatively, in Practitioners (CA,CS,CMA,etc.)e of the third-party application hosted on the premises, the licensing cost may be higher.	✓ Need to pay for the resources that they use, where the price adjusts up or down depending on how much is consumed.
Control	✓ The firm shall retain all their data and are fully in control of what happens to it. Clients / Firms which are in highly regulated industries with extra privacy concerns may prefer on premise solution.	✓ Data and encryption keys reside within your third-party provider, so if the unexpected happens and there is downtime, the firm maybe be unable to access that data
Security	✓ Firms' that have extra sensitive information, must have a certain level of security and privacy that an	✓ Security concerns remain the number one barrier to a cloud computing deployment. There have been many publicized

Key Factor	On-Premise (Traditional Computing)	Cloud Computing
	on-premises environment provides.	cloud breaches, which is a concern across the globe.
Compliance	✓ In Practitioners (CA,CS,CMA,etc.)es of strict regulatory compliance such as Privacy Laws, it is suggested to stay inhouse / on-premise computing	✓ Firms that choose a cloud computing model must do their due diligence and ensure that their third-party provider is compliant with all the different regulatory mandates within their industry
Flexibility	✓ Traditional computing is less flexible and requires Virtual Private Connection (VPN) or remote desktop access connectivity to access it from other locations.	✓ This enables work from anywhere and using any system across any location.
Backup and Recovery	✓ The onus of back up and testing for recovery is on the firm in Practitioners (CA,CS,CMA,etc.)e of the traditional computing technology	✓ The service provider provides almost 99% uptime and regularly backs up the data in addition to testing for recovery.
Software Updates	✓ The updates to the software must be manually done in Practitioners (CA,CS,CMA,etc.)e of traditional computing	✓ The cloud service provider regularly provides updates to the software.

c. Virtual Private Network

This is the technology that typically enables you to “work-from-home” and still ensure the data resides only at one centralised repository. A virtual private network extends a private network, say access to your firm’s resources, across a public network, such as Internet, and the firm to send and receive data across shared or public networks as if their computing devices were directly connected to the firms’ private network.

d. Social Networking and Online communities

Online communities such as Taxguru, LinkedIn provide a platform where people can share and collaborate the knowledge and their experiences. This can also be used to showPractitioners (CA,CS,CMA,etc.)e firm’s ability / expertise in the certain domains such as FEMA, GST, Litigation etc. While on one end, it helps to be updated and socially connected, on the other end, it could also help market, or reach a larger population.

e. Document Management System

This can be referred to as an electronic filing cabinet, where all the data in digitised form is stored, sorted and retrieved. Access restrictions can be placed on who can

access which type of data and it can also track the version and the users who are adding, altering or deleting the data. The data can be stored client wise, year wise, category wise etc. Appropriate tags can be assigned for easy search and retrieval of the data.

f. Communication and Instant Messaging Technology

It is crucial for the firm to communicate regularly and sometimes repeatedly with their employees, clients, prospective clients and the world at large. Technologies such as email, Voice over Internet Protocol (VoIP) or popularly called as Internet calling, are paving way to faster, accurate and quicker communication across borders.

g. Video Sharing and Webinars

From face to face, we are moving towards a technology of screen to face. Video sharing, podPractitioners (CA,CS,CMA,etc.)ts are increasing becoming popular and these enable sharing of videos, audios, over the internet across various location, geographies. This also enables firms to conduct virtual seminars, popularly called as webinars over the internet and thereby gives a global presence for the firm.

h. Blogs

A blog is a website, generally maintained by an individual or the firm, where commentaries or views on a particular subject such as the latest amendment, budget etc, are often shared. The readers may also have options to respond and post their own thoughts / view / queries. This can also be used by the firms to outline new ideas and create an engage with clients and prospects.

i. Knowledge Management Systems

These are systems which have a repository of the firms' research and processes deployed in solving a problem or addressing client requirements for the first time. These are documented in such a way to help the firm in using it with ease subsequently. This can also document various Standard Operating Procedures (SOPs), formats, process narrative etc.

j. Open Source Applications

These are applications / software that are distributed for free or do not have a cost for usage. While the features may be limited, they might be handy in solving a few business problems. Care should be taken to identify the extent to which the firm shall rely on the application as these may have many limitations.

k. Data Analytics and Visualisation

These are tools that cannot analyse large volumes of data and convert them to nuggets of information and insights. They are the tools which help the firm in analysing digital data. Data analytics is the process of examining data sets in order to draw conclusions

about the information they contain, increasingly with the use of technology or specialist software.

It provides an opportunity to expand and deepen the analysis of a client's operations, provides an opportunity to improve the quality and value of audit.

l. Bring your own Device (BYOD)

Bring your own device —also called bring your own technology, refers to being allowed to use one's personally owned device, rather than being required to use an officially provided device. Many of the firms are currently deploying this strategy in their firms to reduce the capital investment. While this brings in flexibility and ease of operations, care should be taken to ensure basic security parameters are installed in addition to data loss prevention solutions.

5. Overview of Hardware Options

Choosing the right platform / hardware requirements is quite a daunting task as the appropriate hardware and operating software combination must be chosen.

The following are the minimum aspects to be considered:

a. Hardware

Majority of the computer systems used in a firm have an Intel based Processor and Microsoft Windows® based operating system. While alternative options such as Apple's Macintosh ("Mac") can be considered, the real challenge is on the compatibility of the Mac with the various accounting and compliance applications. Care should be taken to ensure the licensing norms of the respective software is not violated while decided the hardware for the firm. The firm may be reasonably conservative in choosing the hardware configuration for the systems, as there may not be high-end operations which require huge memory or processing speed.

In general, systems with Intel Core i3 and above or its equivalent, with a minimum RAM of 2GB and Hard disk space of 512 GB is considered a standard configuration. As regards choosing the type of Hard disk, the traditional model of hard disk drive (HDD) which operates on a circular disc, is relatively cheaper compared to the solid-state drive (SSD) which boasts of better processing speed and comes with a slightly premium price.

b. Thin-client Computing / Virtual Machine Computing

The traditional model of computing considers the "fat-client" approach where almost all the systems within the firm would be of similar capabilities. In the traditional fat client-based model, all users have personal computers (PC) on their desks, which are connected to a file server that allows users to share resources such as printers, email, and files. All the applications are installed on the PC. This means that for an office running 15 applications with 10 team members, will require atleast 150 software installations, and hence the name, fat client computing since the PC, is full of all the software the user needs.

In a thin client model, all users log in to one or more central servers running Terminal Services or Citrix. The users do not need the applications installed on their PC. All

software is installed only once on each server and is instantly available to all users. This model may require additional application such as Citrix which enable such virtualisation. Further the compatibility of the applications and other utility software need to be decided.

Given below are some of the factors which can help the firm take decision:

- ✓ Software supplier support for the environment;
- ✓ The need for multi-locations and/or remote access;
- ✓ The ability to source skilled IT professionals to support the environment;
- ✓ Whether critical peripherals will operate;
- ✓ The number and complexity of applications where a thin client environment makes it easier to manage installations and updates;
- ✓ The effect on team members of a more austere computing environment generally delivered in the thin client world; and
- ✓ Cost differences over the life of the system

c. Servers

Servers are critical components of any system. A server failure can cause significant disruption and loss of productivity. Additional expenditure to gain greater assurance of server reliability is a prudent investment. It is preferred to go with curtained branded server manufacturers, since response times for parts and service technicians may be superior.

A key aspect is to configure server hardware with redundant components such as hard disks and power supplies so that, should a failure occur, the operation of the server is not affected.

It is to be noted that the Server system is a system with substantial computing power in comparison with the other workstations. Certain smaller firms may choose to have one of the workstations as a “Server” by marginally increasing its computational power such as RAM or storage space. This model may be suitable for firms having limited teams.

d. Portable workstations

Laptops and tablet computers enable the workstation to be portable and therefore improve productivity. But security and data storage are areas to be addressed. Further, it is recommended to encrypt the data stored on hard disks and implement password enabled security. Further, since they can be easily connected to the Internet via wireless networks, there is high risk of infection from malicious software. Care should be taken to install and maintain software to protect systems from malicious attack.

e. Printers & Scanners

With the printer technology continuously evolving, multi-functional printers which can scan, print, copy and even send emails are available in the market today. Network printers are recommended over the other models as they are connected to the network and any system in the network can access the printer. The other factors to be considered are colour printing, ability to scan multiple pages in a short while, ability to print back to back automatically etc.

f. Networking, Cabling and Switches

Networking and cabling are required while setting up the office. This is normally done while setting up the office. Switches are devices which connects multiple computers and is used to send and receive data over the network. Care should be taken while choosing the type of Switch and the load that it would be able to take.

g. Wireless network and Routers

Wireless networks are increasingly being used, where cabling is difficult or expensive to implement or for teams working at a client's premises or portable workstation. These come with a variety of encryption standards such as WPA/WPA2 to ensure the data is encrypted while transmitting the same. It is also important to ensure that these networks are secure, since wireless networks can be accessed from a remote location by implementing the highest level of security. Wireless networks can be significantly slower than cabled connections. Like other infrastructure, however, speeds and supported distances between devices continue to increase.

h. UPS (Uninterruptible power supply) and Surge protectors

Where power is not reliable, UPS acts as a safeguard by ensuring there is no interruption in power supply even though there is power failure. Power spikes can damage hardware and power outages can cause complete system failure. Therefore, it prudent to have UPS and surge protectors in place. The size and capacity of UPS has been decided based on the number of systems in place and the maximum time for which the backup is necessary in the event of a power failure.

i. Physical Security

Firms may also choose to have access card / biometric based entry and exit to ensure only authorised personnel have physical access to the firm. Care should be taken on how access is given to guests and visitors.

j. Storage Area Network (SAN) / Backup Systems

The firm may prefer keeping dedicated systems / storage area networks exclusively dedicated for storage, backup and recovery. This could be handy to ensure a backup of data is taken as per the policy defined. Alternatively, the firm may choose to perform an online back up using the services of a cloud service provider / SaaS based provider.

k. Information Security

Information Security devices such as Firewall are essential to prevent undesirable access over Firewall. Firewalls, either hardware- or software-based, should be implemented; this limits the traffic that can access the firm's infrastructure. Assessment should also be done with respect to restriction of USB drives / Pen drives within the organisation as these increase the risk of virus attacks and also have a risk of data leakage.

As SMPs Firms deal with critical and confidential data of multiple clients, it is important to ensure security of this data both from external and internal risks. As specific guidance to SMPs Firms, annexures to this book includes security guidelines in brief and detailed. Further, the appendix to this book has sample policy template which can be used as a reference for implementing security as relevant for the firm.

6. Overview of Software Solutions

We are providing a broad overview of the software solutions available for SMPs Firms. Technology solution providers keep on innovating and releasing newer solutions covering hitherto uncovered areas. Hence, it is advisable to explore and identify the software options available, evaluate them and select what is relevant and ensure successful implementation.

a. Operating Systems

Operating systems are the software that bring the computer hardware to life and provide the services that are used by the business software applications. Every computer has an operating system. Microsoft dominates the supply of operating system software to businesses such as accountancy firms. It provides Windows Server software for the system's servers and the desktop Windows operating system for PCs. It is for this environment that the software industry targeting the profession develops its software. It is not recommended that firms move outside the Microsoft world for its operating systems except in special circumstances. Operating system suppliers, particularly Microsoft, provide regular, often weekly, updates to their software. It is critical that these updates are loaded as they often contain changes to close security holes discovered in the system. Even though Microsoft provides an automatic update service, firms should ensure that a manual check is done on a regular basis to ensure the updates are correctly loaded.

b. Productivity and Office Automation Software

Word processing, spreadsheets, calendar, tasks, presentations, and email are the most heavily used applications in any firm. This software is designed to improve productivity in performing everyday tasks. Microsoft office applications are the most popular one in this space. Alternative applications such as OpenOffice.org, Google Docs, Zoho Suite can be considered.

c. Practise Management Software

A practise management software helps the firm in managing the day to day operations of the firm. Starting from efficient work and task allocation and tracking, to automating repetitive tasks, managing timesheets and invoicing to managing receivables, practise management software helps the firm in multiple ways. Some of this software also have an inbuilt additional feature such as Customer Relationship management tools (CRM), bulk email features etc. They also have advanced reporting capabilities including tracking productivity, profitability, billing and performance.

d. Backup

Firms need to back up systems effectively, so that the systems and data can be recovered in the event of a system failure. Every firm must ensure that adequate on-site and off-site backups are maintained. Technology solutions are available at affordable price to do an on-site / off-site backup. Cloud back up technologies may also be explored.

e. Accounting Automation Software

These software in addition to accounting, have features (either inbuilt or as an add-on) which can either automate the data entry process, prepare real time financial statements in compliance with regulatory requirements or prepare monthly MIS based on the needs of the firm / client. They also have interfaces which enable interfaces to assist in efficient downloading and processing of bank statement, automated

accounting, data entry, expense management etc. The modern accounting automation software which are hosted on the cloud have enabled access across geographies and have enabled real-time validation and access restrictions based on roles. These are also compatible over a mobile phone through mobile apps or through mobile version of the websites.

f. Tax Return Preparation Software

These are software which help in preparing the tax returns as per the required statute say Income Tax, GST, Provident Fund etc. This software has an option to enter the data either directly or through interfaces which is in turn validated based on a predefined set of rules.

The output of this is either printed out or uploaded directly into the concerned regulatory website. Most prominent features are: automatic reconciliation, validation, customized checklists, assign specific questions, templates, data storage, etc.

g. Company Secretary / Statutory record keeping software

With increasing requirement from Corporate clients and Corporate Law, Company secretary software has become the need of the hour. It has features such as maintenance of statutory registers, minutes of the meeting, pre-filled e-forms, notice to Board Meeting and Agenda, automated search etc.

h. Audit Automation Software

Automated Audit Planning Software helps the firm to manage the audit universe, risk analysis, audit planning, resource and time management including tracking, field management, maintaining client documentation and issue of audit reports. The features also include options to create/ maintain customized checklists, assign audit questions, templates, data storage and retrieval, etc.

i. Website Hosting of the SMPs Firms

Having firm's domain name makes the entity look professional. If the entity publishes its website through an ISP or a Web hosting site, then there is a URL such as www.yourisp.com/-yourbusiness.This generic address does not inspire confidence in a client like a domain name (www.yourcompany.com) does. Some have engaged web developers to custom build a website. These websites can be difficult to maintain, and update and your firm is locked into the web developer for ongoing maintenance and support.

j. Anti-virus / End Point Protection

Endpoint protection is an approach of detecting malicious network activity and protecting computer networks including servers, desktops, and mobile devices from intrusions and malware attacks. They run in the background and periodically scan device directories and files for malicious patterns indicating the presence of malware. The also prevent suspicious programs from being executed.

k. Chatbots

A computer program designed to simulate conversation with human users, especially over the Internet. It's a piece of software that conducts a conversation via auditory or textual methods. Driven by AI, these are software acts like an assistant that

communicates with us through text messages, a virtual companion that integrates into websites, applications or instant messengers.

I. **Authenticator Apps**
It is a security app that can protect your online accounts against password theft. It's easy to set up and can be used in a process called two-factor authentication (2FA). Through this, in addition to password, an OTP gets generated through the app which can be used as an additional authentication protocol. It may also enable a single sign-on where the users need not remember multiple passwords and login with just one credential, despite using different software.

The next section includes list of software solutions relevant for SMPs Firms which are provided only as reference with no specific recommendations. The list is only illustrative and not exhaustive. SMPs Firms are advised to explore and select what is best suited for them.

IV. Technology Deployment including FAQs on Technology for SMPs Firms

Technology will play a significant role in all modern accounting firms. To achieve this firms must consider the following:

- ✓ Develop a strategic plan and budget for the firm's technologies.
- ✓ The Internet is transforming how firms today are interacting with clients. Consider adopting Cloud based / SaaS based applications.
- ✓ Firm websites are critical components in servicing clients and in positioning the firm for recruitment. It important to have a website which is regularly updated.
- ✓ Firms must ensure adequate technical support is in place for efficient and reliable systems.
- ✓ It is recommended to stick to mainstream hardware and applications that are in wide use so the firm can have confidence that the applications and systems will deliver desired outcomes.
- ✓ Practice management, accounting and audit automation and tax software together with word processing and spreadsheet software are the key production platforms that define the efficiency of the firms.
- ✓ Hardware platforms should be implemented that efficiently and reliably support these applications.
- ✓ Document-management and knowledge-management applications have the potential to deliver significant improvements in client service and efficiency in the future.
- ✓ Implementation and training are the key to successful use of technologies.
- ✓ Adequate attention and resources should be dedicated to risk management to prevent catastrophic failures.

Technology, when used strategically, is a mechanism to improve efficiency. The implementation of new and emerging technologies can completely transform a firm and having a technology and e-business strategy is important for real change to occur.

Technology is an example of an emerging risk which firms need to acknowledge as our business ecosystem continues to face rapid change. Technology is a key component of success in any firm in today's world. It is critical that accountants stay up to date on the solutions available and the benefits these technologies can deliver. It is equally important to dedicate sufficient resources to ensure that any solutions that are deployed are properly implemented and maintained.

To succeed, firms must ensure that people fully understand and capitalize on the functionality of the software. All staff will need to be well trained to ensure the promised productivity gains from any solution are achieved.

1. List of software / Tools to automate office

The Committee for Members in Practice of ICAI has tie up with various software companies for getting the best software for SMPs Firms at best possible terms. You can refer to the latest list of software available under this option from the committee's website: https://cmpbenefits.icai.org/. The list of software available is not comprehensive but this can be referred before buying the software to consider the pricing and terms.

The software available for SMPs Firms covering various areas keeps on increasing day by day. Most of the SMPs Firms are familiar with software solutions as they use them in their office. Hence, instead of providing list of specific software. We have provided indicate list of software covering each of the specific areas of automation from the DCMM 2.0 guide. The list is only illustrative and not recommendatory.

The best approach to find right software solution for your firm is to get information from peers who have implemented, research online, see a demo, discuss with team and implement.

List of Software referenced in DCMM 2.0 Version			
Sec.	**Reference Sheet**	**Tool/ Website name Name**	**Purpose**
A	Managing Digital Identity	1. Domain.com 2. GoDaddy.com 3. Bluehost.com 4. HostGator.com	Create Domain Mail IDs
A	Operational Process Automation	1. GreytHR 2. PeopleSoft Absence Management 3. Cuckoo Tech	Attendance and leave management systems
A	Operational Process Automation	1. Teramind 2. Actimo 3. CurrentWare etc.	Employee monitoring software
A	Operational Process Automation	1. Basecamp 2. Staffbase 3. Zoom Video Communications 4. Jostle 5. Blue Jeans 6. Skype etc.	Internal communication-chats/instant messaging
A	Operational Process Automation	1. Dropbox Business 2. Amazon 3. Google Drive for Work etc.	Centralized file storage system/server
A	Operational Process Automation	1. Kissflow 2. Dapulse 3. ProWorkFlow 4. Papilio 5. CCH iFirm. Etc.	Workflow management

AJA #NEWTHINKING

A	Operational Process Automation	1. PeopleWorks 2. 247HRM 3.Pocket HRMS	HR Tools
A	Operational Process Automation	1. Freshdesk and many others	Knowledge management
A	Operational Process Automation	1. JazzHR 2. Interview Coordinator 3. Google forms	Interview management
A	Operational Process Automation	1. Salesforce 2. Zoho 3. Hubspot	CRM tool/system
A	Operational Process Automation	1. Quickbooks 2. Slickpie 3. Quantum Invoicing	Invoicing and receivable management
A	Electronic Payments	1.Google Pay 2.Phone Pe 3.Paytm	Electronic payment options
A	Online scans for adverse content	1. Hootsuite2. Social Mention3. Sprout Social4. TweetReach	Social media monitoring
B	Digital Etiquette	1. Firm newsletter 2. Bulletin boards 3. On-line quizzes / tests 4. Off-site training camps etc	Digital etiquette Awareness
B	Protecting against digital threats	1. DLP (Data Loss Protection) technique 2. Bitlocker.	Cyber-security threats
C	Use of Automated Audit Planning Software	1. Audit Automation by CCH 2. Audit Management Solution by Metric Stream 3. Audit management software by Risk Pro 4. Audit management software by Gensuite	Audit management tools
C	Use of Automated Audit Planning Software	1. SimplifyPractise 2. Papilio 3. Cordl 4. ProCAAT	Workflow management
C	Use of External Automated Audit Tools for Data Extraction, Sampling, Analytics, etc.	1. eCAAT 2. Power BI 3. Tableau 4. Knime 5. R etc.	Data Extraction, sampling and other analysis
C	Use of External Automated Audit Tools for Data	1.eCAAT 2. Power User 3.Kutools	Advanced Excel / Add-ins for Analysis

AJA #NEWTHINKING

	Extraction, Sampling, Analytics, etc.		
C	Use of External Automated Audit Tools for Data Extraction, Sampling, Analytics, etc.	1. QuickBooks 2. Zoho Books 3. Cloud based CRM Tools 4. Online Invoicing Tools like Wave Apps etc	SaaS based tools
C	Use of in-built audit tools/capabilities in client-side applications like ERPs	Audit tools within the ERP	Use of in-built audit tools
C2	Use of Automated Taxation Planning Software	1 Reylon for taxes 2. Winman for taxes 3. Saral for taxes 4. Cleartax for taxes 5. Gen CompLaw for Secretarial 6. CimplyFive for Secretarial	Tax and compliance management tools
C2	Use of Automated Taxation Planning Software	1. SimplifyPractise 2. Papilio 3. Cordl 4. ProCAAT	Customize / alter general workflow management tools
C3	Use of Automated Accounting Software	1. QuickBooks 2. Tally TDLs 3. E2Tally-soft 4. Tally Customization applications	Specific to automation of accounting:
C3	Use of External Automated Accounting Tools for Data Entry, Sampling, Analytics, etc.	1. QuickBooks 2. Zoho Books 3. Cloud based CRM Tools 4. Online Invoicing Tools like Wave Apps	SaaS based tools
C4	Use of Automated Software for rendering management Consultancy Services	1. Tools of SAP Oracle 2. Power BI 3. eCAAT 4. Macros and Statistical Function in Excel	Assist in rendering management consultancy services, share projection & modelling
C4	Use of Automated Software for rendering management Consultancy Services	1. SimplifyPractise 2. Papilio 3. Cordl 4. ProCAAT	Workflow management tools
C4	Use of External Automated Management Consultancy Services Tools for rendering various services	1. eCAAT 2. Power BI 3. Tableau 4. Knime 5. R etc.	Data Extraction, sampling and other analysis

AJA #NEWTHINKING

D	Use of Advanced and Emerging Technologies	1. QuickBooks 2. Tally TDLs 3. E2Tally-soft 4. Tally Customization applications	Automation of accounting
D	Use of Advanced and Emerging Technologies	1. Botkeeper 2. vic.ai 3. ai-accountant 4. Legalmation premonition.ai 5. Mindbridge.ai	AI Tools
D	Use of advanced technology and communication media	1. Flow XO 2. Beep Boop 3. Bottr 4. Motion.ai	Build chatbots

The next section includes annexure and appendix providing a variety of sample templates, checklists, guidelines and references. These may be referred and adapted as required.

V. Sample Templates, Checklists and useful references

1. Annexure-1: IT Strategic plan Template

In developing an IT strategic plan, it is advisable to use a standard template. Template of a typical IT strategic plan with specific sections and overview of details is given below. This may be adapted as required by the firm:

1. **Introduction**: The introduction will provide an overview of the mission, vision, strategy and goals of the firm and highlight the importance/benefits, processes and the approach adapted in developing the IT strategic plan.

2. **IT vision**: Based on overall vision of the firm, the IT vision will outline the technology plan and will include overview of the current technology deployment and the planned technology deployment to meet the overall strategic requirements.

3. **IT strategic issues**: The key IT strategic issues which need to be addressed such as optimal technology infrastructure, outsourcing, internal/external requirements, security, contingency planning, change management, organisation structure, impact, risk management strategy, etc. are included in this section.

4. **IT policy and principles**: This section will include the policies/ principles which are developed to guide the use of information technology. This will include information security policy to be implemented in the firm. Some key principles are:
   a. Development must use flexible systems concepts to ensure integration, connectivity and compatibility,
   b. Development shall address the needs of all internal and external customers, architectures must reflect existing standards,
   c. Employees shall have access to the technology, data and applications required to do their jobs as effectively as possible,
   d. Technologies are supported throughout their he IT plan consider the aspirations and objectives of the SMPs Firms and take into account the external factors such as:
      i. Potential avenues for growth
      ii. Growth of existing clients
      iii. Acquisition of new clients
      iv. Envisaged expected competition in the traditional areas, and
      v. Regulatory requirements that will impact and influence development of practice.
      vi. The process life cycle and information architecture developed for delivering the service and for exchange of information shall be appropriate, flexible and adaptable to change.

5. **Technology portfolio:** This section will provide a summary of current technology deployment at various layers of technology as applicable for the firm such as network, servers, operating systems, database, office automation applications, etc.

6. **Application portfolio**: This section will include summary of all major applications deployed in the enterprise, relevant vendors and related business processes, IT application software and in each of the key areas and related responsibilities.

7. **IT Software application software and assignments of responsibilities**. This section will outline the processes for managing the IT Application software and responsibilities assigned for managing them. This will include definition of the recommended list of IT functions, identify whether these are centralised or distributed and list the specific functions with assigned responsibility and role as responsible, accountable, consulted or informed.

8. **List of strategic projects, and project descriptions**: This section will outline list of strategic IT Project which is planned to be implemented with specific milestones and timelines. Details of project plans with related initiatives have to be planned, implemented and monitored till they are successfully deployed.

9. **Some tips and guidelines:** Allocate time for planning sessions as required. It is important to make appointments for yourself and stick to it. Involve your key staff and take inputs from them. It will be very useful if you treat your firm as an important client so that you remain objective and provide the right priority. section provides an overview of allocation of resources.

10. **Some Examples**: Some examples of planning for IT projects are:
    a. Maintenance Activities are allocated 30% of the available programming hours.
    b. Enhancement Activities are allocated 20% of available programming hours.
    c. New Project Development is allocated 50% of available programming hours.
    d. Each of the projects could be listed with their project types.
        i. Information Technology Project Types or Business Process Project Types.
        ii. The projects could be classified as:
            1. Active Projects,
            2. On-hold/Pending Enhancements,
            3. Idea Statement or Business Practitioners (CA,CS,CMA,etc.)e.

11. **Sample project format:** A listing of the projects may be provided in the following format:
    a. Project Type
    b. Project Name
    c. Current Priority
    d. Project Description
    e. Business Practitioners (CA,CS,CMA,etc.)e reference and whether Business Practitioners (CA,CS,CMA,etc.)e is developed.
    f. Details of each of the projects are provided as per project plan template.

2. Annexure-2: Security Guidelines (Do and Don't's)

DO:

1. Realise your personal responsibility with regard to information security
2. Inform yourself about the established security rules; apply them and, if unclear, seek guidance
3. Be aware of what can go wrong and be alert to what does go wrong
4. Report security incidents and concerns about:
    a. Access violations
    b. Inadequate backups
    c. System unavailability
    d. Poorly controlled or error-prone electronic transactions
5. Make regular backups of critical data and test the backups made.
6. Change your password immediately upon receipt and then regularly in accordance with policy. Ensure that the chosen password is difficult to guess.
7. Return all company materials, including data files, upon termination of employment
8. Lock rooms when leaving important data or equipment behind
9. Remember that anything you write in an e-mail may be held against you or your enterprise
10. Dispose of sensitive information effectively—shred, wipe disks, destroy media, etc.

DO NOT:

1. Misuse enterprise computing resources for unapproved purposes (e.g., intellectual property protection violations, illegal content)
2. Leave the system unattended and accessible for extended periods of time
3. Tell anyone your password or share it with anyone (except properly authorised group passwords)
4. Disclose sensitive data to anyone who is not authorised to receive it or who does not need to know it
5. Load or use pirated software or unqualified shareware onto any enterprise computer
6. Bypass established network connection rules
7. Bypass or de-install virus checking software
8. Bypass or de-install virus recovery software
9. Ignore security incidents
10. Be negligent with sensitive information put into your care (on portable media, e.g., CD, DVD, flash/pen media, PDA and laptops)
11. Introduce and/or remove computing equipment without authorisation

3. Security Guidelines (Brief)

TASK	DESCRIPTION
1. Passwords	• Ensure your passwords are strong and secure • Use multi factor authentication where possible • Constantly change passwords, and do not share them.
2. System Access	• Remove system access from people who no longer need it, and limit access to only those needed to do their role. • Administrator privileges are provided on an 'as-needs' basis. • Review access and roles regularly.
3. Secure Wi-Fi & Devices	• Secure your wireless network and be careful when using public wireless networks with mobile devices. • Avoid transacting online where you are using public or complimentary Wi-Fi. • Never leave your information physically unattended – secure your electronic devices. • In Practitioners (CA,CS,CMA,etc.)e of operating from remote, educate employees to protect their Wi-fi devices.
4. Legitimate Software	• Only download/install programs from a trusted source. • Consider using application whitelisting so only authorised software applications run on your computer. • Disable untrusted Microsoft Office macros and block or uninstall Flash and Java. • Strictly avoid pirated software
5. Patches and Anti-Virus	• Ensure all mobile devices/operating systems/software have the latest available security updates and run weekly anti-virus/ malware scans. • A patch management solution may be able to help.
6. 'Clean' devices	• Do not use USB or external hard drives from an unfamiliar source. • Disable USB drive in all systems except where required.
7. Social Media	• Be vigilant about what you share on social media – try to keep personal information private and know who interact with online. • Educate employees, interns and families on the same.

TASK	DESCRIPTION
8. Email	• Use a spam filter for your email and use email carefully - be wary of downloading attachments or opening links in emails you have received in Practitioners (CA,CS,CMA,etc.)e it is a 'phishing' attempt.
9. Daily backup	• Use off-line, incorruptible, and disconnected backups. • Cloud based backup solutions can be preferred. • External Hard disks are also good options.

4. Annexure-4: Security Guidelines (Checklist)

The senior management of SMPs Firms should be very well conversant with information security policy and related guidelines. Given below is a illustrative list of guidelines which will be useful as a quick reference guide for Owners/Partners, Managers to verify and confirm compliance. This list can be updated and used as a checklist to implement/confirm compliance with security in a SMPs Firms.

1. Ensure that all team members know who does what relative to security—the security dos and don'ts.
2. Ensure that staff has sufficient resources and skills to exercise its security responsibilities.
3. Ensure that security is considered in job performance appraisals and results in appropriate rewards and disciplinary measures.
4. Ensure awareness of the need to protect information; provide training to operate information systems securely and be responsive to security incidents.
5. Ensure that security is considered while procuring/installing existing/new software.
6. Ensure that staff with sensitive roles has been vetted.
7. Ensure that the firm is not dependent on any one individual for any key security task (i.e., appropriate segregation of duties).
8. Ensure that privacy and intellectual property rights, as well as other legal, regulatory, contractual and insurance requirements, have been identified with respect to security and processes in your area of responsibility.
9. Ensure that applicable security measures have been identified and implemented (e.g., effective backup, basic access control, virus detection and protection, firewalls, intrusion detection and adequate insurance coverage).
10. Ensure that a suitable technical environment is in place to support security measures.
11. Ensure that staff knows how security measures operate and has integrated them in day-to-day procedures.
12. Ensure that key users have safely and regularly tested security measures in a representative environment.
13. Establish rules for authorizing changes and for evaluating their security impact.
14. Ensure that security aspects have been considered in all service level agreements and the security competence of the service providers has been assessed.
15. Ensure that risks of dependency on security service providers have been assessed and mitigated.
16. Ensure that on-call support, backup, resilience and continuity have been established for IT services supporting critical office functions.
17. Ensure that users know what to do in Practitioners (CA,CS,CMA,etc.)e critical IT services are unavailable.
18. Ensure that access control and connectivity rules for internal and external users have been implemented, based on office needs and risks.
19. Ensure that security administration has been enabled and resourced with procedures and service levels to identify users and assign, activate, maintain and eventually remove access rights.

20. Ensure that incident management procedures are defined and in effect to ensure that relevant security incidents (access control violations, viruses, illegal use of software, hacking, etc.) are identified, monitored, analysed and acted upon.
21. Ensure that the security baseline and vulnerabilities have been constantly assessed through monitoring system weaknesses—intrusion detection, penetration and stress testing, and testing of contingency plans.
22. Ensure that there is a measurable and management-transparent security strategy based on benchmarking, maturity models, gap analysis, and continuous performance monitoring and reporting.
23. Ensure that security guidance and contractual obligations for use of digital signatures, e-commerce and electronic payments exist.
24. Ensure that an up-to-date list of hardware and software critical for important IT services is maintained, including the disaster backup site.
25. Ensure that archiving and backup procedures for critical information have been defined and implemented.
26. Ensure that important computing equipment is safe from theft, damage, or loss, e.g., put cables on laptops, lock computer rooms and know the location of media devices.
27. Ensure that applying a high level of control has hardened all security and critical server and communications platforms.
28. Ensure that operating system versions have been continuously kept up to date as soon as feasible.
29. Ensure that physical protections (e.g., parameter security for heat, dust and electricity) are in place.
30. Ensure that adequate security has been implemented for wireless communications systems and is monitored continuously.
31. Where appropriate, ensure that competent external resources have reviewed the information security control mechanisms, and assessed compliance with laws, regulations, and contractual obligations relative to information security. Leverage their knowledge and experience and act upon their suggestions.
32. Ensure that clear, pragmatic enterprise and technology continuity programs have been established, continually tested and kept up to date.
33. Ensure that critical office processes and supporting infrastructures are resilient to failure, especially targeting single points of failure.
34. Ensure that the usage of computers is monitored for compliance with established rules of appropriate usage.
35. Ensure that the organisation has been kept informed of new threats (e.g., viruses) and has been included in regular risk assessments.
36. Ensure that mobile computing devices have been included in the security strategy and have been protected, for example: Laptops, PDAs, etc., are protected from theft and physical damage, and stored data are protected from disclosure.
37. Portable media (e.g., optical, memory) are protected.
38. Ensure that use of social media by the staff is in compliance with firm's policy.
39. Ensure that the IPR of software used is complied and no unauthorized software are installed on office computers.
40. Ensure that all staff are trained and well-conversant with security policies and procedures of the company and they have provided written confirmation in agreed format.

5. Annexure-5: Work from Home / Virtual Office Checklist

Domain	Points to be considered
Data Protection	• Avoid personal email for work • Watch out for Phishing attacks • Remind staff NOT to open links or documents with Coronavirus information or any such information • Don't share work files using personal cloud storage accounts on Googledrive, Dropbox, OneDrive, etc. • If you use personal devices, limit work-files to one folder. Delete it once you transfer the files • Enable two-factor authentication • Install approved anti-malware and install the latest updates • Encrypt/ password-protect external USB storage. • Use company VPN if available. Check with office policies before start using collaboration apps/ services • Wherever necessary, encrypt the key computer systems • Ask staff to back up their data on an approved external hard disk that is NOT permanently connected to the device • Encourage employees to have their Wi-Fi devices at home secure and protected. WPA2 Encryption is recommended.
Employees	• Communicate the policies and procedures • Regularly educate and train them on the various risks • Request employees to update the software on their home routers and personal devices • Update hardware inventory - refresh the list of devices used from home • Mandate two-factor authentication for all employees • Run mandatory training to discuss at home privacy and security risk scenarios • Inform employees to take regular breaks after working for a few hours. • Set up a time zone for personal and office life • Regularly schedule meetings with your team and interact. • Host various fun based activities to keep the employees active and energetic. • Encourage them to regular exercise and keep themselves fit. • Ensure the workplace where employees work regularly is well lit, and is ergonomically well fit. • Ask staff NOT to defer critical updates to software • Remind staff NOT to lend their machines to their children or other members of the family • Stress the IMPORTANCE of NOT sharing passwords • Educate all staff to ensure webcams are blocked by default

Domain	Points to be considered
	• Educate staff on the Dos and Don'ts's of Video conferencing. • Remind staff NOT to leave their machines UNLOCKED, especially during a call or when visiting the washroom • Do Not Mix Work and Personal Accounts
IT Resources	• Ensure adequate licences are in place for employees working from home • Discourage employees downloading software / freeware • Install end point security and mobile device management resources • Deploy tools for connecting remotely such as VPN, remote desktop etc. • Video conferencing and office communication apps to be installed for easier communication. • Office management tool can be used for updating the daily tasks regularly. • Back up of all key resources to be regularly performed. • Ensure cloud-based tools are in place to assist the firm in operating remotely • Virtual Desktop options can also be considered. • Compatibility of the cloud-based applications / virtual desktop systems with that of on-premise systems to be verified.

AJA #NEWTHINKING

6. Annexure-6: SOP for Conference Calls during Work from Home

I. Technical checks:

1. Ensure good internet connectivity and power back up.
2. Keep the Video conferencing application ready to use beforehand.
3. Test the audio and video before the call starts.
4. Test links and files to be shared before the calls.
5. Keep device adequately charged before the call.
6. Know how to share screen to present or show files.

II. Responsibilities

1. Ensure a clean background and an adequately lit place.
2. Dress appropriately and maintain decorum.
3. Find a quiet place to avoid background noise.
4. Keep diary, pen, Cell phones, chargers, relevant Acts / books ready
5. Use earphones if required to avoid disturbance to others around.
6. In Practitioners (CA,CS,CMA,etc.)e of multiple participants, indicate when you want to speak to avoid confusion.
7. No Con-calls from public places
8. Ensure Client confidentiality while discussing over con-call.

III. Punctuality:

1. Send meeting invite well in advance if you are the coordinator.
2. Log-in on time and adhere to the meeting timings.

IV. Concluding the call:

1. Summarize and recap at the end of the meeting.
2. Capture the minutes of the meeting and follow up or update.

7. FAQs on Technology for Practitioners (CA,CS,CMA,etc.)

1. ***What are the minimum IT Requirements for a SME Firm?***
    - Desktop / Laptop computers, where one of which can act as a Server
    - Network and LAN Switch
    - Microsoft Windows License (alternative Operating System may be considered, depending upon the acceptability and requirements)
    - Productivity Applications such as Microsoft Office (Microsoft 365 which is subscription-based model is recommended at least for the key employees).
    - Open source productivity applications like Open Office, LibreOffice, WPS office can be considered, if the firm is constrained on cost
    - Accounting, Tax, Compliance solutions based on the firm requirements
    - End Point or anti-virus software solutions.
    - Regular updates to software and security patches
    - Email ID for all members. Domain based email ID is preferred over generic (ex: user@cafirm.org)
2. ***What are the minimum requirements for going to be a virtual firm?***

    In addition to requirements in FAQ-1, the following are suggested:

    - VPN Connection to access the office infrastructure and on-premise software
    - Remote working tools like Any Desk, Zoho Assist, Virtual Desktop etc.
    - Cloud-based accounting and compliance tools
3. ***What is the minimum security required for a SMPs Firms?***
    - Anti-virus Software
    - Strong Wi-fi Encryption (WPA2)
    - End-point protection solution (optional, instead of anti-virus software)
    - Firewall Software / Hardware Solution (optional)
4. **Should a SMPs Firms have a Privacy Policy?**

    Yes, as the SMPs Firms processes Sensitive personal data such as passwords, Bank Account details, Credit/debit card details. Further as per the Information Technology Act, 2002 (as amended 2008) and The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, every entity dealing with sensitive personal data should have a privacy policy and indicate how they process the same.

5. **What are the minimum IT Policies to be adopted?**

While this is fully optional, the following are recommended:

- IT Security Policy – outlines the overall security
- Acceptable Usage Policy – policy on how IT assets should be used
- Access control Policy – policy on how the access controls would be governed
- Password Policy – policy on how the password is configured and frequency at which it is required to be changed.

6. ***How can I adopt to emerging technology?***
    - Many of the existing products we use (example Microsoft 365) has built-in features of Artificial Intelligence in them. One should try to start using them to begin their journey of adoption of emerging technology.
    - Multiple tools are also available for analysing data such as eCAAT, tCAAT (Tally CAAT), PowerBI (from Microsoft), Zoho Analytics etc.

7. ***What is BYOD Policy?***

    It is concept where employees bring their own assets for office. Example could be employees bringing in their own laptops for the office use. Many firms adopt this to reduce the capital expenditure. Few other firms may procure the laptop and recover the cost (partly or in full) from the employee throughout the tenure of the employment or internship. In all such Practitioners (CA,CS,CMA,etc.)es, the firm will have to formulate a BYOD Policy on how the asset and data should be safeguarded. The following should be addressed:

    - Device types which will be supported. Ex: Smartphones, tablets, laptops etc.
    - How will employees connect to the network? Will virtual private networks (VPNs) and virtual desktops be required?
    - What applications and websites will be blacklisted?
    - Which work resources can the device access?
    - Will access to public Wi-Fi networks be forbidden? Unless the device is equipped with a VPN, connecting over a public network is risky.
    - What steps should employees take when their device is lost or stolen?

8. **Minimum security requirements for BYOD Policy?**

    In Practitioners (CA,CS,CMA,etc.)e of BYOD policy, the following are recommended security requirements:

- Mobile Device Management Solution which can encrypt and wipe off the data in Practitioners (CA,CS,CMA,etc.)e the employee loses the asset
- Identity and access management solution to ensure only authorised users login
- Access controls restriction from installing unauthorised software

9. Do I require a firewall?

Even though it is not mandatory, it is recommended to install a firewall where there is a local server. This will protect from unauthorised access.

10. Do I require a corporate domain email ID?

Consider the privacy and the confidentiality of the information SMPs Firms deal with, it is recommended to have a domain email. (user@cafirm.org). this will ensure the sensitive data is well protected and safeguarded.

11. What is office management software?

These are a suite of products which create a workflow and can enable the SMPs Firms track the overall tasks, assign tasks, monitor tasks and maintain the leave and track the employee records.

VI. Appendix-1: Sample Policy Template for SMPs Firms

Brief overview of Sample Policy

When Technology is deployed, there are inherent risks which need to be mitigated. SMPs Firms deploy technology and deal with digital data which belongs to their clientele. Hence, ensuring security of this information is extremely critical. This requires adapting right security policy which is relevant for the firm.

For SMPs Firms which intend to operate virtually or already operating virtually, the need for security becomes much critical as information is accessed not only from office location where security measures might be implemented but information is accessed, processed and exchanged between clients and various staff of SMPs Firms from any location. Implementing right level of security for various types of information exchange has to be planned, documented, communicated and implemented.

The sample policy template covers diverse areas of security policy. This is not comprehensive but illustrative. It can be adapted/updated as per specific requirements of the firm. Most firms may have implemented security in their own way and many firms may not have documented it. This policy template can be used as quick reference guide to identify specific sections which are relevant and use it for documenting, communication, training and adaptation as a policy. Further, detailed procedures as per specific technology deployment can be added under relevant sections as required.

1. Introduction

A. Scope

This document details the policy and guidelines for the information security within <SMPs Firms>. The security policy and guidelines specified here applies to the protection of the information assets of <SMPs Firms information assets) and its clients (client information assets). It is an umbrella policy that is supplemented by more detailed and technical policies, standards, and guidelines as required. As a policy document, it is intended to present a complete picture on <SMPS FIRMS>'s approach to security.

B. Goals

The goals of the of the security program are:

a. **Avoidance:** The ability to prevent unauthorized access to client information assets and <SMPS FIRMS> information assets (together referred to as corporate information assets)
b. **Assurance:** The compliance with policies, standards, and guidelines to ensure the protection of the corporate information assets.
c. **Continuity:** The ability to guarantee that disaster recovery plans have been developed and tested.

All new hires within <SMPS FIRMS> will be required to read the security policy as applicable to their role and confirm their understanding with security policy. Each of them will be required to sign a legally binding agreement committing conformance with the Security policies of <SMPS FIRMS>.

C. Risks to assets within <SMPS FIRMS>

The risks to the above information assets include:

a. **Risk to confidentiality:** The risk that sensitive data will be accessed by an unauthorized party and/or prematurely disclosed.
b. **Risk to data integrity:** The risk of unauthorized modification to data such as financial information or product specifications.
c. **Risk to availability:** The risk that critical systems cannot be accessed in a timely manner, resulting in delayed processing.
d. **Risk to repudiation:** The risk that an individual can deny sending or receiving a message. This can also be referred to as accountability
e. **Risk to privacy:** A risk related to a corporations' unauthorized use, disclosure, or gathering of user personal information.

D. Controls

Controls are to be designed to govern the following actions:

i. Confidentiality

Access is granted to assets and information on need to do and need to know basis based on specific roles and responsibilities as assigned from time to time. All employees are expected to maintain strict confidentiality of information in their custody and share it only as authorised and required as per their job requirements.

ii. Integrity

The completeness and correctness of information is to be maintained at all stages or processing of information. All employees are expected to ensure that this is confirmed in all the software they are using.

iii. Repudiation

Clients may deny requests for modification to the data. The same may be true of operators of the system. Digital signature will be used with encryption as required to ensure non-repudiation of key exchange of office communication/documents as per policy.

iv. Availability

The availability of information in hard copy or digital format is to be used to all users as and when required for performing the work. This will be used that required information is protected against system failures by having appropriate back up and redundant systems as per back up policy of the <SMPs Firms>.

v. Authorization and access control

Different users play different roles in usage of the applications. Discretionary access control is required based on roles. All employees have to use discretion in ensuring that access controls and security are implemented by maintaining secrecy of passwords.

vi. Non-repudiation

There are potential costs in a client being able to deny a specific action such as stop payment for an employee. It must not be possible to repudiate such actions. Digital signature and other encryption devices/mechanism will be used by employees of <SMPS FIRMS> as required.

2. Information Security Policy

This section of Information Security Policy sets forth some important rules relating to the use of <SMPS FIRMS> computers and communications systems. These systems include individual PCs, Laptops, Tablets, PDAs, Cell Phones, etc. provided to employees, centralized computer equipment, all associated software, and <SMPS FIRMS>'s telephone, cell phones, voice mail and electronic mail systems.

<SMPS FIRMS> has provided these systems to support its mission. Although limited personal use of <SMPS FIRMS>'s systems is allowed, subject to the restrictions outlined below, no use of these systems should ever conflict with the primary purpose for which they have been provided, <SMPS FIRMS>'s ethical responsibilities or with applicable laws and regulations. Each user is personally responsible to ensure that these guidelines are followed.

All data in <SMPS FIRMS> computer and communication systems (including documents, other electronic files, e-mail and recorded voice mail messages) are the property of <SMPS FIRMS>. <SMPS FIRMS> may inspect and monitor such data at any time. No individual should have any expectation of privacy for messages or other data recorded in <SMPS FIRMS> systems. This includes documents or messages marked "private," which may be inaccessible to most users but remain available to <SMPS FIRMS>. Likewise, the deletion of a document or message may not prevent access to the item or eliminate the item from the system.

Security procedures in the form of unique user sign-on identification and passwords have been provided to control access to <SMPS FIRMS> host computer system, networks and voice mail system. In addition, security facilities have been provided to restrict access to certain documents and files for the purpose of safeguarding information.

3. Security Risks (Don'ts for employees)

The following activities, which present security risks, should be strictly avoided.

a. Attempts should not be made to bypass, or render ineffective, security facilities implemented by the <SMPs Firms>.
b. Passwords should not be shared between users. If written down, Password should be kept in locked drawers or other places not easily accessible.
c. Documents of other users should not be browsed unless there is a legitimate reason to do so.
d. Individual users should never make changes or modifications to the hardware configuration of computer equipment. Requests for such changes should be directed to computer support team through Head of Department.
e. Additions to or modifications of the standard software configuration provided on <SMPS FIRMS> PCs should never be attempted by individual users (e.g., autoexec.bat and config.sys files). Requests for such changes should be sent through the Head of Department.
f. Individual users should never load personal software (including outside email services) to <SMPs Firms> computers. This practice risks the introduction of a computer virus into the system. Requests for loading such software should be directed to computer support or the Director.
g. Programs should never be downloaded from any websites or copied from other computers outside the <SMPs Firms> onto <SMPs Firms> computers.

h. Downloading or copying such programs also risks the introduction of a Computer virus. If there is a need for such programs, a request for assistance should be directed to computer support or management. Downloading or copying documents from outside the <SMPs Firms> may be performed not to present a security risk.
i. Users should not attempt to boot PCs from USBs or other hardware. This practice also risks the introduction of a computer virus.
j. <SMPS FIRMS>'s computer facilities should not be used to attempt unauthorized access to or use of other organizations' computer systems and data.
k. Computer games should not be loaded on <SMPS FIRMS> PCs or computer systems.
l. Unlicensed software should not be loaded or executed on <SMPS FIRMS> PCs. <SMPs Firms> software (whether developed internally or licensed) should not be copied onto other hardware other than for the purpose of backing up your hard drive.

4. Ownership/Documentation of assets given to employees

a. All assets provided by <SMPs Firms> to employees including computers/laptops and accessories with details of system configuration and software installed will be noted in a separate register or file.
b. A signed document will be obtained from the employee for the assets received by them for use for performing <SMPs Firms> work.
c. These documents are to be taken on record and in Practitioners (CA,CS,CMA,etc.)e of employee leaving the job, the assets are to be taken back in working condition or in Practitioners (CA,CS,CMA,etc.)e of damage, the relevant cost as applicable has to be recovered from the employee.
d. All client/work related file including original files and work outputs are the assets of the <SMPs Firms> and the employee shall maintain these in strict confidentiality as assets of the <SMPs Firms> in safe custody.
e. These files shall be handed over or shared as authorised to authorised staff. The employee does not have any right over the original or work output and these files and related work documents are IP of the <SMPs Firms>.

5. Authorisation of users

a. Computers/laptops handed over to employees will be first created with admin rights for which user id should be maintained by IT manager with a copy maintained by the owner/manager/partner as authorised.
b. Specific user should be created for the employee with rights allocated as required as per authorisation of the specific computer/laptop to the employee.
c. Rights of installation of new software will be restricted so that only authorised software is installed in the software
d. New software will be installed only with written authorisation of the head of department and as per requirements. This software will be installed by the system administrator.

6. Acceptable Use Policy

A. Overview

The objective of the IT department of <SMPS FIRMS> for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to <SMPS FIRMS>'s established culture of openness, trust and integrity. IT Security is committed to protecting <SMPS FIRMS>'s employees, clients and other stakeholders involved from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of <SMPS FIRMS>. These systems are to be used for office purposes in serving the interests of the <SMPs Firms> and of clients during normal office operations.

Effective security is a team effort involving the participation and support of every <SMPS FIRMS> employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

B. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at <SMPS FIRMS>. These rules are in place to protect the employee and <SMPS FIRMS>. Inappropriate use exposes <SMPS FIRMS> to risks including virus attacks, compromise of network systems and services, and legal issues.

C. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct <SMPS FIRMS> office or interact with internal networks and office systems, whether owned or leased by <SMPS FIRMS>, the employee, or a third party. All employees, vendors, consultants, temporary, and other staff at <SMPS FIRMS> and other associates of the <SMPs Firms> are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with <SMPS FIRMS> policies and standards, and applicable laws and regulation.

This policy applies to employees, vendors, consultants, temporaries, and other staff at <SMPS FIRMS>, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by <SMPS FIRMS>.

D. General Use and Ownership

<SMPS FIRMS> proprietary information stored on electronic and computing devices whether owned or leased by <SMPS FIRMS>, the employee or a third party, remains the sole property of <SMPS FIRMS>.

a. Employees must ensure through legal or technical means that proprietary information of <SMPS FIRMS> is adequately protected.
b. Employees have a responsibility to promptly report the theft, loss or unauthorized disclosure of <SMPS FIRMS> proprietary information.
c. Employees may access, use or share <SMPS FIRMS> proprietary information only to the extent it is authorized and necessary to perform your assigned job duties.
d. Employees are responsible for exercising good judgment regarding the reasonableness of personal use.

E. Security and Proprietary Information

a. System level and user level passwords must comply with the Password guidelines. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
b. All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.
c. Postings by employees from an <SMPS FIRMS> email address on social media should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of <SMPS FIRMS>, unless posting is in the course of office duties.
d. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

7. Internet Acceptable Use Policy

A. Overview

Internet connectivity is an imperative need, but it presents the <SMPs Firms> with new risks that must be addressed to safeguard the firm's vital information assets.

These risks include:

a. Access to the Internet by personnel that is inconsistent with office needs results in the misuse of resources. These activities may adversely affect productivity due to time spent using or "surfing" the Internet. Additionally, the <SMPs Firms> may face loss of reputation and possible legal action through other types of misuse.
b. All information found on the Internet should be considered suspect until confirmed by another reliable source. There is no quality control process on the Internet, and a considerable amount of its information is outdated or inaccurate.
c. Access to the Internet will be provided to users to support office activities and only on an as-needed basis to perform their jobs and professional roles.
d. Desktop access to the Internet is provided to employees when there is a necessity and the access has been specifically approved. <SMPS FIRMS> has provided access to the Internet for authorized users to support its mission. No use of the Internet should conflict with the primary purpose of <SMPS FIRMS>, its ethical responsibilities or with applicable laws and regulations.
e. Each user is personally responsible to ensure that these guidelines are followed. Serious repercussions, including termination, may result if the guidelines are not followed.

<SMPS FIRMS> may monitor usage of the Internet by employees, including reviewing a list of sites accessed by an individual. No individual should have any expectation of privacy in terms of his or her usage of the Internet. In addition, <SMPS FIRMS> may restrict access to certain sites that it deems are not necessary for office purposes.

B. Purpose

The purpose of this policy is to define the appropriate uses of the Internet by <SMPS FIRMS> employees and affiliates.

C. Scope

The Internet usage Policy applies to all Internet users (individuals working for the <SMPs Firms>, including permanent full-time and part-time employees, contract staff, temporary agency staff, partners, managers and vendors) who access the Internet through the computing or networking resources. The <SMPs Firms>'s Internet users are expected to be familiar with and to comply with this policy and are also required to use their common sense and exercise their good judgment while using Internet services.

D. Internet Services Allowed

*Internet access is to be used for office purposes only***.** Capabilities for the following standard Internet services will be provided to users as needed:

- **E-mail**: Send/receive E-mail messages to/from the Internet (with or without document attachments).
- **Navigation**: WWW services as necessary for office purposes, using a hypertext transfer protocol (HTTP) browser tool. Full access to the Internet; limited access from the Internet to dedicated <SMPs Firms> public web servers only.
- **File Transfer Protocol (FTP)**: Send data/files and receive in-bound data/files, as necessary for office purposes.
- **Online Storage Facility**: For storing/sharing files of clients for work done and related documents.
- **Communication Software**: For online meetings with office team/clients as required.

Management reserves the right to add or delete services as office needs change or conditions warrant. ***All other services will be considered unauthorized access to/from the Internet and will not be allowed.***

E. Request & Approval Procedures

Internet access will be provided to users to support office activities and only as needed to perform their jobs.

F. Request for Internet Access

As part of the Internet access request process, the employee is required to read both this Internet usage Policy and the associated Internet/Intranet Security Policy The user must then sign the statements official confirmation accepting that he/she understands and agrees to comply with the policies. Users not complying with these policies could be subject to disciplinary action up to and including termination. Confirmation by signing the acknowledgment form, is required before access will be granted.

G. Approval

Internet access is requested by the user or user's manager submitting an ***IT Access Request*** form to the concerned department along with an attached copy of a signed Internet usage Coverage Acknowledgment Form.

H. Removal of privileges

Internet access will be discontinued upon termination of employee, completion of contract, end of service of non-employee, or disciplinary action arising from violation of this policy. In the Practitioners (CA,CS,CMA,etc.)e of a change in job function and/or transfer the original access code will be discontinued, and only reissued if necessary and a new request for access is approved.

All user IDs that have been inactive for thirty (30) days will be revoked. The privileges granted to users must be re-evaluated by management annually. In response to feedback from management, systems administrators must promptly revoke all privileges no longer needed by users.

I. Policy

i. Resource Usage

Access to the Internet will be approved and provided only if reasonable office needs are identified. Internet services will be granted based on an employee's current job responsibilities. If an employee moves to another office unit or changes job functions, a new Internet access request must be submitted within 5 days.

User Internet access requirements will be reviewed periodically by <SMPs Firms> departments to ensure that continuing needs exist.

ii. Allowed Usage

Internet usage is granted for the sole purpose of supporting office activities necessary to carry out job functions. All users must follow the corporate principles regarding resource usage and exercise good judgment in using the Internet. Questions can be addressed to the IT Department.

Acceptable use of the Internet for performing job functions might include:

- Communication between employees and non-employees for office purposes;
- IT technical support downloading software upgrades and patches;
- Review of possible vendor web sites for product information;
- Reference regulatory or technical information from regulatory/related websites.
- Visiting website of statutory/accounting/ICAI -national/regional/local branches.
- Research on specific area of work as required.

iii. Personal Usage

Using <SMPs Firms> computer resources to access the Internet for personal purposes, without approval from the user's manager and the IT department, may be considered cause for disciplinary action up to and including termination.

All users of the Internet should be aware that the <SMPs Firms> network creates an audit log reflecting request for service, both in-bound and out-bound addresses, and is periodically reviewed.

Users who choose to store or transmit personal information such as private keys, credit card numbers or certificates or make use of Internet "wallets" do so at their own risk. The <SMPs Firms> is not responsible for any loss of information, such as information stored in the wallet, or any consequential loss of personal property

iv. Prohibited Usage

Information stored in the wallet, or any consequential loss of personal property.

Acquisition, storage, and dissemination of data which is illegal, pornographic, or which negatively depicts race, sex or creed is specifically prohibited.

The <SMPs Firms> also prohibits the conduct of any personal service, political activity, engaging in any form of intelligence collection from our facilities, engaging in fraudulent activities, or knowingly disseminating false or otherwise libellous materials.

a. Employees should safeguard against using the Internet to transmit personal comments or statements through e-mail or to post information to news groups that may be mistaken as the position of <SMPS FIRMS>.
b. Employees should guard against the disclosure of confidential information using Internet e-mail or social media.
c. Employees should not download personal e-mail or Instant Messaging software to <SMPS FIRMS> computers.

Other activities that are strictly prohibited include, but are not limited to:

a. Accessing <SMPs Firms> information that is not within the scope of one's work. This includes unauthorized reading of client account information, unauthorized access of personnel file information, and accessing information that is not needed for the proper execution of job functions.
b. Misusing, disclosing without proper authorization, or altering client or personnel information. This includes making unauthorized changes to a personnel file or sharing electronically, client or personnel data with unauthorized personnel.
c. Deliberate pointing or hyper-linking of <SMPs Firms> Web sites to other Internet/WWW sites whose content may be inconsistent with or in violation of the aims or policies of the <SMPs Firms>.
d. Any conduct that would constitute or encourage a criminal offense, lead to civil liability, or otherwise violate any regulations, local, state, national or international law including without limitations US export control laws and regulations.
e. Use, transmission, duplication, or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets, or patent rights of any person or organization. Assume that all materials on the Internet are copyright and/or patented unless specific notices state otherwise.
f. Transmission of any proprietary, confidential, or otherwise sensitive information without the proper controls.
g. Creation, posting, transmission, or voluntary receipt of any unlawful, offensive, libellous, threatening, harassing material, including but not limited to comments based on race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.
h. Any form of online gambling.

The following activities are also strictly prohibited:

i. Unauthorized downloading of any shareware programs or files for use without written authorization in advance from the user's manager.
j. Any ordering (shopping) of items or services on the Internet except at a minimal level as may be required.
k. Playing of any games.
l. Forwarding of chain letters.
m. Participation in any on-line contest or promotion or acceptance of promotional gifts.

<SMPS FIRMS>'s facility of connection to the Internet provide to the employees for performing office work, may not be used for any of the following activities:

v. System and Network Activities

The following activities are strictly prohibited, with no exceptions:

a. Violations of the rights of any person or <SMPs Firms> protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by <SMPS FIRMS>.
b. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which <SMPS FIRMS> or the end user does not have an active license is strictly prohibited.
c. Accessing data from a computer system or server or an account for any purpose other than conducting <SMPS FIRMS> office, even if you have authorized access, is prohibited.
d. Copying/installing software, technical or product information in violation of international or national or state laws, is illegal.
e. Introduction of malicious programs in <SMPS FIRMS>'s computer systems (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) is liable for legal action.
f. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
g. Using an <SMPS FIRMS> computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
h. Making fraudulent offers of products, items, or services originating from any <SMPS FIRMS> account.
i. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
j. Circumventing user authentication or security of any host, network or account.
k. Introducing honeypots, honeynets, or similar technology on the <SMPS FIRMS> network.
l. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
m. Providing information about, or lists of, <SMPS FIRMS> employees to parties outside <SMPS FIRMS>.

vi. Email and Communication Activities

a. When using <SMPs Firms> resources to access and use the Internet, users must realize they represent the <SMPs Firms>. Whenever employees state an affiliation to the <SMPs Firms>, they must also clearly indicate that "the opinions expressed are

my own and not necessarily those of the <SMPs Firms>". Questions may be addressed to the IT Department

b. Sending unsolicited email messages, including the sending of "junk mail" or any other material to anyone who did not specifically request such material (email spam).
c. Any form of harassment via email, telephone or SMS, WhatsApp or any other means, whether through language, frequency, or size of messages.
d. Unauthorized use, or forging, of email header information.
e. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
f. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
g. Use of unsolicited email originating from within <SMPS FIRMS>'s networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by <SMPS FIRMS> or connected via <SMPS FIRMS>'s network.
h. Posting the same or similar non-office-related messages on social media such as Facebook, twitter, linked in, WhatsApp, Instagram, etc.

vii. Blogging and Social Media

a. Blogging by employees, whether using <SMPS FIRMS>’s property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and ocPractitioners (CA,CS,CMA,etc.)ional use of <SMPS FIRMS>’s systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate <SMPS FIRMS>’s policy, is not detrimental to <SMPS FIRMS>’s best interests, and does not interfere with an employee's regular work duties. Blogging from <SMPS FIRMS>’s systems is also subject to monitoring.
b. <SMPS FIRMS>’s Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any <SMPS FIRMS> confidential or proprietary information, trade secrets or any other material covered by <SMPS FIRMS>’s Confidential Information policy when engaged in blogging.
c. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of <SMPS FIRMS> and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by <SMPS FIRMS>’s Non-Discrimination and Anti-Harassment policy.
d. Employees may also not attribute personal statements, opinions or beliefs to <SMPS FIRMS> when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of <SMPS FIRMS>. Employees assume any and all risk associated with blogging.
e. Apart from following all laws pertaining to the handling and disclosure of copyrighted or materials, <SMPS FIRMS>’s trademarks, logos and any other <SMPS FIRMS> intellectual property may also not be used in connection with any blogging activity

The above policy guidelines will be updated as and when required by the <SMPs Firms>. All employees are expected to adhere to the latest policy as applicable.

Employees having any questions regarding any of the policy guidelines listed in the information security policy may contact their IT/Administration Manager, or the Director.

8. Software Licensing/IPR policy

The <SMPs Firms> strongly supports strict adherence to software vendors' license agreements. When at work, or when <SMPs Firms> computing or networking resources are employed, copying of software in a manner not consistent with the vendor's license is strictly forbidden. Questions regarding lawful versus unlawful copying should be referred to the IT Department for review or to request a ruling from the Legal Department before any copying is done.

Similarly, reproduction of materials available over the Internet must be done only with the written permission of the author or owner of the document. Unless permission from the copyright owner(s) is first obtained, making copies of material from magazines, journals, newsletters, other publications and online documents is forbidden unless this is both reasonable and customary. This notion of "fair use" is in keeping with international copyright laws.

Using <SMPs Firms> computer resources to access the Internet for personal purposes, without approval from the user's manager and the IT department, may be considered cause for disciplinary action up to and including termination.

Users who choose to store or transmit personal information such as private keys, credit card numbers or certificates or make use of Internet "wallets" do so at their own risk.

a. Employees shall use only licensed software provided by <SMPs Firms>. If they require any new software, written request should be sent through head of department with purpose of usage. Employees should not be downloaded from the Internet as the download could introduce a computer virus onto <SMPS FIRMS>'s computer equipment. In addition, copyright laws may cover the software so the downloading could be an infringement of copyright law.
b. <SMPS FIRMS> strictly prohibits use of any downloaded software other than licensed software providing the <SMPs Firms>. In Practitioners (CA,CS,CMA,etc.)e any employee has downloaded the software, they shall be personally responsible for violation of copyright laws and the consequences thereof. The <SMPs Firms> is in any way responsible for such violation of copyright laws.
c. <SMPS FIRMS> will acquire required software as specified and approved while buying computers.
d. A standard hardware/software policy will be developed for identifying specific computer configuration with standard software as required by different roles within the <SMPs Firms>. This will consider the designation, role and responsibility and work requirements of each of the employee required to use computer.
e. Software will be procured and installed as officially approved for specific role and installed by IT manager and documented.
f. Employees will provide written undertaking that they will not install any unapproved software on the system allocated to them for office work. If any deviation to this policy is found, the specific employee is legally responsible and appropriate action will also be taken by the <SMPs Firms>.

9. Password Selection and Change Requirements

Password selection and change requirements are two of the most important parts of an effective security program. Therefore, <SMPS FIRMS> systems must meet the following password selection and change requirements:

a. User passwords must consist of atleast 8 characters which is a combination of numeric, lower and upper Practitioners (CA,CS,CMA,etc.)e and special characters
b. System and administrative accounts' passwords must use a complex password.
c. User passwords must not contain the user's name or ID.
d. Passwords shall not be communicated in a manner other than from the security function to the user directly when it is assigned or changed.
e. If a user is provided with an initial password, this password must be changed the first time a user logs into a system.
f. Users must log on using default password and change password immediately.
g. Before a password change takes effect, users must be required to enter their new password multiple times.
h. User password resets must only be performed when requested by the individual to whom the user ID is assigned. The relevant office unit should be responsible for verifying the identity of the user.
i. Password for user accounts must expire after a maximum of 90 days and a new password must be created. The same password must not be selected more than once in 90 days.
j. Passwords for system and administrative accounts must expire after a maximum of 60 days and a new password must be created. A give password must not be used more than once in 90 days.
k. Clear-text user ID and passwords must not be stored in database. They must be encrypted using appropriate software as applicable.
l. Default passwords shipped with software and hardware must be disabled or changed immediately.
m. Generic accounts and group passwords must not be allowed so that individual accountability is maintained at all times.

10. Meeting Operational Security Requirements

Operational security requirements address the controls required to sustain normal office operations.

A. Physical and Environmental Protection

Controls are necessary to protect the facilities that house <SMPS FIRMS> system resources against physical and environmental threats for continued operation. The requirements for physical and environment protection are as follows:

a. <SMPS FIRMS> must ensure protection for its computer networks, systems, digital devices to ensure continuity of operations against environmental factors such as fire, dust, power, excessive heat and humidity.
b. Procedures need to exist for facilities management to monitor and test fire-suppression system equipment at least every six months and document test results.
c. All <SMPS FIRMS> IT security personnel must be trained in the use of any automatic fire-suppression systems, the use of portable fire extinguishers, and in the proper response to smoke and fire alarms.
d. UPS and batteries for running them must be provided and tested on a regular basis.
e. Food and drink must be prohibited in the workplace and near computers to prevent damage and spillage.

AJA #NEWTHINKING

B. Physical Access Control

All <SMPS FIRMS> Information facilities should have appropriate physical access controls in place to protect information assets from unauthorized access.

a. <SMPS FIRMS> must physically secure <SMPs Firms>'s computer system, laptops, digital devices and related components which is in their custody to ensure safety of these assets.
b. As part of a periodic third-party review of access controls, the <SMPS FIRMS> corporate audit department should commission a reviewer to review automated access control audit trails and visitor logs for appropriateness.
c. <SMPS FIRMS> must provide adequate building security to protect the entire facility during off-hour periods.
d. All <SMPS FIRMS> facilities must have regular monitoring of the access control system on site or must be connected to a monitoring station that is manned during office and non-office hours as appropriate.
e. All IT security systems must have self-contained battery backup and should work in a networked environment or stand-alone as needed.

11. Accounting and Maintenance of Records

<SMPS FIRMS> will manage I & T assets through their life cycle to make sure that their use delivers value at optimal cost, they remain operational (fit for purpose), and they are accounted for and physically protected.

<SMPS FIRMS>'s policy is to ensure that those assets that are critical to support service capability are reliable and available. <SMPS FIRMS> will manage software licenses to ensure that the optimal number are acquired, retained and deployed in relation to required office usage, and the software installed is in compliance with license agreements.

<SMPS FIRMS> will manage assets from procurement to disposal and also ensure that assets are utilized as effectively and efficiently as possible and are accounted for and physically protected until appropriately retired.

a. <SMPs Firms> as a <SMPs Firms> will maintain fixed assets register covering all the assets of <SMPS FIRMS> including tangible and intangible assets. This register will be maintained as per specified format with separate category for each type of assets. All purchases and write-off of assets will be updated on regular basis.
b. Computers/software licenses as and when purchased are to be debited to fixed assets or software license or expense accounts as appropriate as per accounting policy.
c. The fixed assets of <SMPS FIRMS> are to be physically verified, reconciled with the accounts and assets which are obsolete are to be written off. The physical verification will cover all the computer desktop/laptops and the software licenses purchased and paid for by the <SMPs Firms>.
d. Based on the results of verification any difference between the books and actuals will be reconciled and appropriate action taken. Further, this will be updated in a fixed assets register.
e. Software licenses purchased should be identified and stored in a separate folder in both physical and digital format as part of record for proving conformation with IPR as required.
f. Insurance will be taken for all the assets of <SMPS FIRMS> including computers assets on the book value or realisable value whichever is lower. Insurance has to be obtained for

all the assets as per category of the assets to ensure that <SMPs Firms>'s assets are protected against loss.

g. Software licenses purchased annually are to be accounted as SW license expenses. In Practitioners (CA,CS,CMA,etc.)e of software purchased with lifetime license, then they may be written off over a period of 3 years of estimated life.

h. AMC/ASC paid for software is to be accounted under relevant head and charged off during the year based on period applicable. In Practitioners (CA,CS,CMA,etc.)e of software license fees paid extending beyond the financial year, amount applicable for next year to be considered as pre-paid expenses and charged as expenses in next financial year.

12. Email Policy

A. Overview

Electronic email is pervasively used in almost all industry verticals and is often the primary communication and awareness method within an organization. At the same time, misuse of email can post many legal, privacy and security risks, thus it's important for users to understand the appropriate use of electronic communications.

B. Purpose

The purpose of this email policy is to ensure the proper use of <SMPS FIRMS> email system and make users aware of what <SMPS FIRMS> deems as acceptable and unacceptable use of its email system. This policy outlines the minimum requirements for use of email within <SMPS FIRMS> Network.

C. Scope

This policy covers appropriate use of any email sent from a <SMPS FIRMS> email address and applies to all employees, vendors, and agents operating on behalf of <SMPS FIRMS>.

D. Policy

a. All use of email must be consistent with <SMPS FIRMS> policies and procedures of ethical conduct, safety, compliance with applicable laws and proper office practices.
b. <SMPS FIRMS> email account should be used primarily for <SMPS FIRMS> office-related purposes; personal communication is permitted on a limited basis, but non-<SMPS FIRMS> related commercial uses are prohibited.
c. All <SMPS FIRMS> data contained within an email message or an attachment must be secured according to the policy of the <SMPs Firms> by using password/relevant security as required. This password will be shared in a separate email/messaging platform.
d. Email should be retained only if it qualifies as a <SMPS FIRMS> office record. Email is a <SMPS FIRMS> office record if there exists a legitimate and ongoing office reason to preserve the information contained in the email.
e. Email that is identified as a <SMPS FIRMS> office record shall be retained according to <SMPS FIRMS> Record Retention Schedule.
f. The <SMPS FIRMS> email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any <SMPS FIRMS> employee should report the matter to their supervisor immediately.
g. Users are prohibited from automatically forwarding <SMPS FIRMS> email to a third-party email system Individual messages which are forwarded by the user must not contain <SMPS FIRMS> confidential or above information.
h. Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to perform office work unless specifically authorised. They will not create or memorialize any binding transactions, or to store or retain email on behalf of <SMPS FIRMS>. Such communications and transactions

should be conducted through proper channels using <SMPS FIRMS>-approved communication channel.

i. Using a reasonable amount of <SMPS FIRMS> resources for personal emails is acceptable, but non-work-related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from an <SMPS FIRMS> email account is prohibited.
j. <SMPS FIRMS> employees shall have no expectation of privacy in anything they store, send or receive on the <SMPs Firms>'s email system.
k. <SMPS FIRMS> may monitor messages of employees without prior notice. Employees are not expected to expect privacy for email messages sent through official email id.

13. Disaster Recovery Plan and Back up

A. Overview

Since disasters happen so rarely, management often ignores the disaster recovery planning process. It is important to realize that having a contingency plan in the event of a disaster gives <SMPS FIRMS> a competitive advantage. This policy requires management to financially support and diligently attend to disaster contingency planning efforts. Disasters are not limited to adverse weather conditions. Any event that could likely cause an extended delay of service should be considered.

B. Purpose

This policy defines the requirement for a baseline disaster recovery and back up plan to be developed and implemented by <SMPS FIRMS> that will describe the process to recover IT Systems, Applications and Data from any type of disaster that causes a major outage.

C. Scope

This policy is directed to the IT Management Staff who is accountable to ensure the plan is developed, tested and kept up to date. This policy is solely to state the requirement to have a disaster recovery plan, it does not provide requirement around what goes into the plan or sub-plans.

Key Considerations of Plan:

- **Data Study**: Detail the data stored on the systems, its criticality, and its confidentiality.
- **Criticality of Service List**: List all the services provided and their order of importance. It also explains the order of recovery in both short-term and long-term timeframes.
- **Data Backup and Restoration Plan**: Detail which data is backed up, the media to which it is saved, where that media is stored, and how often the backup is done. It should also describe how that data could be recovered.
- **Equipment Replacement Plan**: Describe what equipment is required to begin to provide services, list the order in which it is necessary, and note where to purchase the equipment.

After creating the plans, it is important to practice them to the extent possible. Management should set aside time to test implementation of the disaster recovery plan. Table-top

exercises should be conducted annually. During these tests, issues that may cause the plan to fail can be discovered and corrected in an environment that has few consequences.

D. Data Backups

This section of Data Back-ups is extracted and adapted from the ICAI Publication: "Office Management Manual for Members in Practice" published by Committee for Members in Practice (CMP), ICAI. The above manual covers following sections.

1. Client relationship management
2. Human resource management including articles management
3. Technology management
4. Assignment management
5. Virtual office management

Regular backups

It is a good practice to take regular backups to prevent any loss of data due to system failure or any contingencies like fire, etc.

Backup destinations

(a) Internal hard disk
(b) External disk

Daily back-ups will be taken on internal hard disk with programmed and scheduled backup, maybe during lunch time or post office time or pre office time. Servers also have Mirror Hard Disks so that every data saved on the Server is mirrored on the Mirror Hard-disk. Back up on external media will be taken once a week and stored at a place away from main office may be in a locker or residence of a Partner to avoid any data loss in Practitioners (CA,CS,CMA,etc.)e of a fire or such other contingencies.

Scheduling a Backup

Software is available for scheduling auto backup at regular intervals. It can be programmed so that archived files (old files) can be backed up once a month and active files can be backed up on daily basis (may be twice daily – depending upon peak or off-peak season). Further it can also be programmed to take incremental backup which means that only additional data created will be backed up to the old backup and hence the old backup will get updated.

Grandfather – Father – Son technique

The Backup should not overwrite earlier backup. There should be a system to create two new backups and there after the earlier one can be overwritten so that at any point of time, the entity has two previous backups intact. Just in Practitioners (CA,CS,CMA,etc.)e the error files get backed up, the old backups can be used.

Data Storage and Retrieval

- The purpose of storage of data is to easily retrieve the same when needed. The Data storage should be so structured that it follows standard nomenclature as well as design and structure of the hierarchy. No individual person can determine the name of the file, folder, sub folder and so on.
- The files should first be distinguished between those for archival and current.
- All Archive files for past period or closed jobs to be saved in separate area marked for the same. The said files should be write-protected, and no person should be allowed to modify any files in archive area.
- To access any files from archived area, first it is to be brought to the current working area with authorisation and then allowed to be edited. The same should be saved with different name and not overwrite any archived data.

- Drop Box or online storage facility as approved by the <SMPs Firms> will be provided to employees for storing/sharing the files as required. These files can be accessed by authorised staff to access these uploaded files from the stored location. A simple procedure of copying the file to drop box and retrieval can be followed. Any member of that group can retrieve and upload files in the said box.

The Disaster recovery plan, at a minimum, should be reviewed an updated on an annual basis. <SMPS FIRMS> will develop detailed procedures for each area of operations in consulting with the operational manager as per their specific requirements.

E. Disposal of Sensitive Material

a. When <SMPS FIRMS>-restricted, confidential, and internal materials are disposed of, it is important to ensure that information is not improperly disclosed or available to un-authorised persons.
b. Computers or laptops will hard-disk, if disposed should be degaussed to ensure that <SMPS FIRMS>'s data is not recoverable using any other utility software.

F. Ensuring Availability of computers

a. <SMPS FIRMS> has formulated this documented procedure for regular monitoring of use of computers.
b. Regular monitoring of usage will include checking whether usage of computers is for office use only, installation of regular updates and installation of any unauthorised software such as gaming/video or other software from unauthorised sites which has high risk of virus attacks and is against policy of <SMPS FIRMS>.
c. Anti-virus software will be procured and installed on all computers/laptops and ensured that these are regularly updated.

14. Work from Home policy

A. Scope

As work from home is becoming new normal, <SMPS FIRMS> has formulated policy for this. This will be circulated, and acceptance of the policy will be confirmed by employees. All employees of the <SMPS FIRMS> are expected to ensure adherence to this policy.

B. Purpose

Working from home has its pros and cons. The challenges include technical and technological know-how, separating personal and work lives when they occur in the same physical space and learning to focus and stay on task without direct supervision. If enterprises will have to understand these challenges and strategize to work around them, it's easy to overcome them and thrive.

C. Overview

A few points to keep in mind while working from home include be alert to advanced technology, always keep security in mind, always stay in touch with colleagues and clients, put in more than regular hours, create a separate working space and if that is not possible then create a designated area which is only for work. This will go a long way in ensuring you are focused and in work mode in that area. While it's uncertain how long current practices will stay in effect, this could be a paradigm shift in office practices in getting work done. The current pandemic

scenario has made it imperative for enterprises to promote working from home. Shifting to a home working environment opens the door to personal devices and applications being used to distribute corporate assets and information. This increases the risk of confidential data being intercepted.

<SMPs Firms> will update and enforce data security and corporate policies to address the use of personal devices for office purposes. This policy is to enable employees to be prepared and provide guidance and advice ahead of time. Apart from the regular policies pertaining to security policy of acceptable using policy of using internet, email, etc. are applicable, this is additional policy and guidelines pertaining to working from home.

The following contents on "Use of Technology" and Guidelines for Work-for-Home" is extracted and adapted from the ICAI Publication: "Office Management Manual for Members in Practice" published by Committee for Members in Practice (CMP), ICAI. The above manual covers following sections and could be referred for more details.

1. Client relationship management
2. Human resource management including articles management
3. Technology management
4. Assignment management
5. Virtual office management

D. Use of Technology

a. <SMPS FIRMS> may use specific technologies like VoIP which enables employees to work from home or anywhere to stay connected to <SMPS FIRMS>, by accessing resources and exchanging information with other staff from remote locations. The technology also enables more opportunities for staff to work from home ("remote working").
b. <SMPs Firms> is using "thin client" environments which enable all staff to access <SMPS FIRMS> 's systems and work as though they are in the office, regardless of actual location.
c. Document management systems are critical to enable access for all files as required. Currently, at <SMPS FIRMS>, a form of remote working is the mobile team member. Equipped with a laptop or netbook, these remote staff can work from any location—home or clients' offices.
d. This also enables employment of staff seeking opportunities to work flexible hours or work from home. There are concerns about supervising employees to ensure productivity is maintained.
e. Working from home requires personal discipline, a quiet work area free of disruption, and all the enabling technology.

E. Some Useful Tools

<SMPs Firms> may useful relevant technology and tools which enable and empower employees for working remotely. These technologies which will enable operating virtual office/work used currently by the <SMPs Firms> are given below.

a. Online backup through Cloud
b. Virtual Call answering service
c. Facility for web conferencing
d. Cloud Hosted application programs
e. Tools for collaboration
f. Online Practice management

g. Cloud Communication app

Employees are expected to learn how to use these technologies safely and securely to perform their office work and to be productive.

F. Suggested Guidance/Rules for Work from Home

Traditionally, <SMPS FIRMS> has been at the forefront of adopting new Technologies. Some of the important Points under consideration for developing Work- from-Home policy are:

a. **IT Infrastructure**: Robust IT infrastructure is required to implement Work- from- Home Policy. IT Infrastructure includes both hardware and software. <SMPS FIRMS> in future will implement robust IT Infrastructure based on the need of work from home policy. Developing IT infrastructure is not one-day job. It will be planned meticulously based on <SMPS FIRMS>'s vision. This will consider: Use of Laptops, Internet Connectivity at office and at employee places (homes), Firewall, antivirus software, Data Security, Data confidentiality, Data Storage, Servers at Office, Cloud Computing, Application Software like accounting soft wares, ability of those software, compliances software for direct tax, GST, other laws, like state tax laws and corporate laws and other software as required.
b. **Employee / Staff**: Check out the list of self-motivated people, do detailed review of set of people who are interested in work from home. The employees or set of people will be with different skill sets to complete the specific job.
c. **Work Tasks:** <SMPS FIRMS> will prepare a list of tasks which can be done from home only. While preparing the list, <SMPS FIRMS> will consider the type of work, confidentiality of the work to be allocated, and client's permission to the work under WFH policy, if required.
d. **Negative list of Work:** <SMPS FIRMS> will also develop negative list of work. The work which is covered under negative list will not be allocated under work-from-home policy. The negative list of work will be circulated to managers/supervisors so that they are aware of the kind of work that will not be covered under work from home policy.
e. **Planning Work**: Once the work list is final, <SMPS FIRMS> will prepare proper chart of work to be done under WFH policy. While preparing the chart, <SMPS FIRMS> will take into consideration timeline / deadline to finish the work, scope of work, review mechanism, skill sets required by the staff to complete the work.
f. **Delegation of Work:** Once the scope of work, time-line skill sets required are identified, the next step is to allocate the work to employees based on different skill sets.
g. **Controlling of Work**: One manager/team leader will be appointed. They are responsible for proper planning of the work, communication between different teams working from home. They will be responsible for ensuring that all the teams on the job allocated are working on timeline already finalised.
h. **Review of Work /Review Mechanism:** Manager/Team leader will decide the review mechanism based on the job time lines. Review of work will be daily, weekly, fortnightly, monthly, quarterly as required.
i. **Team Leader:** Team leader's position will preferably be in the office premises. Team leader may be single point contact between client and different teams.

j. **Training of Team**: Additional training modules will be developed for work-from-home teams. Team training calendar which is set up and followed up meticulously. All employees will be trained or will have to get self-trained to demonstrate the ability to work independently and without supervision or with remote supervision to achieve required outcomes/results.

k. **Upgradation of IT Infrastructure**: Based on assessment of requirements of work to be performed by each of the employees, IT infrastructure will be provided/upgraded to perform work as specified on time.

l. **Infrastructure with Employee**: <SMPS FIRMS> will develop policy for additional capital investment in IT Infrastructure for use by employee at their premises. Bring-your-own-Device (BYOD policy) will be developed and employees compensated as required for using their personal resources for performing work.

m. **Standardization in Hardware configuration / Application Software**: As per work requirements of employees of <SMPS FIRMS> and cost consideration, long term policy will be developed, implemented and continuously monitored for standardization of various computer hardware, software, and service providers to meet needs for performing WFH by employees from different locations.

n. **Employee responsibility for data security**: Employees are expected to comply and adhere to security policy and procedures as laid down to preventing hacking, virus attacks and other threats to data security. All security precautions must be exercised by employees to avoid any damage to confidentiality, misuse of data etc.

o. **Signing of NDA**: When the nature of work is such that it may result in breach of Non-Disclosure Agreement with client and a special permission may be required from the client for carrying out the work from home in Practitioners (CA,CS,CMA,etc.)e of such clients, then additional NDA will be signed by employees.

p. **Regular Communication**: <SMPS FIRMS> will ensure regular communication to employees as to which circumstances, <SMPS FIRMS> will adopt WFH policy. A few examples:

    i. Exceptional situation where one is prevented from attending office, like lockdown due to pandemic or any such similar reasons.
    ii. The WFH arrangement would enhance or maintain productivity.
    iii. There is a benefit to <SMPS FIRMS>, Employee, client without causing loss to either party.
    iv. There would be no significant additional expenses incurred.
    v. Working from home is an approved condition of employment; and/or there are valid personal or family reasons
    vi. There are no alternatives other than using work-from-home due to circumstances which prevent employees to come to office for work.

The Information Security policy of <SMPS FIRMS> is a living document and will be updated on a regular basis as approved by the board, to ensure that it continues to meet the office and regulatory requirements. The document will be made available in hard/soft copy to the employees as required for performing their work.

15. Template: Employee Receipt and Acceptance of IS Policy

I hereby acknowledge having read the Information Security policy of <SMPS FIRMS>. I understand that it is my continuing responsibility to know the latest update to the security policy. I also understand and agree that the adherence to information security policy is valid not only for the duration of my employment contract but also extends to future for any violations found in future after termination of employment.

I have read, understood, and agree to comply with the above requirements of <SMPS FIRMS>. I have also read and understood the <SMPS FIRMS>'s Information Security Policy and agree to continually abide and adhere to it.

Signature: _____

Print Name: _____

Place: _____

Date: _____

AJA #NEWTHINKING

16. Useful References:

This section contains a sample list of useful references relating to technology implementation for SMPs Firms. This list is indicative and is provided only to serve as useful reference for doing further research.

A. ICAI

1. DIGITAL COMPETENCY MATURITY MODEL FOR PROFESSIONAL ACCOUNTING FIRMS - VERSION 2.0 AND IMPLEMENTATION GUIDE

https://resource.cdn.icai.org/57964daaab47265.pdf

2. Guide to Cloud Computing

https://resource.cdn.icai.org/56801icaidaabcloud.pdf

3. Concept paper on Blockchain Technology

https://resource.cdn.icai.org/51416daab41119.pdf

4. Concept Paper on embracing Robotic Process Automation

https://resource.cdn.icai.org/51008daab230718-1110.pdf

5. Office management Manual for members in practice

https://resource.cdn.icai.org/60284cmp49102.pdf

6. Guide To Working From Home For Every Professional

https://www.wirc-icai.org/members/wirc-publications/guide-to-working-from-home-for-every-professional

7. Tally for Professionals

https://www.wirc-icai.org/images/publication/Tally-Full-Book.pdf

B. From IFAC

1. Preparing Future Ready professionals:

https://www.ifac.org/knowledge-gateway/preparing-future-ready-professionals/discussion/how-secure-your-client-s-data

2. Small business continuity checklist – How to survive and thrive Post Covid-19

https://www.ifac.org/system/files/publications/files/Small-Business-Survive-Post-COVID-19.pdf

3. Guide to Practice Management for Small- and Medium-Sized Practices, 4th Edition

http://www.ifac.org/system/files/publications/files/PM-Guide.pdf

4. Companion Manual

http://www.ifac.org/system/files/publications/files/Companion-Manual.pdf

5. Planning your firm

http://www.ifac.org/system/files/publications/files/Module-1.pdf

6. Practice models

http://www.ifac.org/system/files/publications/files/Module-2.pdf

7. Building and Growing your firm

http://www.ifac.org/system/files/publications/files/Module-3.pdf

8. People power: Developing a People Strategy

http://www.ifac.org/system/files/publications/files/Module-4.pdf

9. Leveraging Technology

http://www.ifac.org/system/files/publications/files/Module-5.pdf

10. Client Relationship Management

http://www.ifac.org/system/files/publications/files/Module-6.pdf

11. Risk Management

http://www.ifac.org/system/files/publications/files/Module-7.pdf

12. Succession Planning

http://www.ifac.org/system/files/publications/files/Module-8.pdf

13. Practice Transformation Action Plan

http://www.ifac.org/system/files/publications/files/Practice-Transformation-Action-Plan.pdf

14. Understanding and communicating value creation

http://www.ifac.org/system/files/publications/files/PAIBC-Meeting-Report-Nov-2019.pdf

15. Future-Ready Accountants in Business
https://www.ifac.org/system/files/publications/files/Future-Ready-Accountants-in-Business.pdf

16. Re-imagining Accountancy's Future

https://www.ifac.org/knowledge-gateway/developing-accountancy-profession/discussion/cpa-canada-reimagining-accountancy-s-future

17. Knowledge Gateway – Resources from IFAC for SMPs Firms
https://www.ifac.org/knowledge-gateway

18. Meaningful work for the digital professional: roadmap beyond the pandemic

https://www.accaglobal.com/gb/en/professional-insights/technology/Meaningful_Work_Digital_Professional.html

C. AICPA

Practise Management
https://www.aicpa.org/content/dam/aicpa/interestareas/personalfinancialplanning/resources/pfppracticemanagement/downloadabledocuments/technology-for-planning.pdf

Info Security
https://www.aicpa.org/content/dam/aicpa/interestareas/privatecompaniespracticesection/qualityservicesdelivery/informationtechnology/downloadabledocuments/top-22-cyber-checklist.pdf

D. CPA Australia

1. Guide to Cloud Accounting

https://www.cpaaustralia.com.au/-/media/corporate/allfiles/document/professional-resources/business/guide-to-cloud-computing.pdf?la=en&rev=9faec59d6ed24374a809ed2b08ddaf20

1. Disaster Recovery Toolkit

https://www.cpaaustralia.com.au/-/media/corporate/allfiles/document/professional-resources/business/disaster-recovery-toolkit

2. Developing policies and procedures for your business

https://www.cpaaustralia.com.au/-/media/corporate/allfiles/document/professional-resources/business/developing-policies-and-procedures-for-business.pdf?la=en&rev=87e856caac0f4e1dbc3e6b1428044068

E. Harvard Business Review

3. A Guide to Managing Your (Newly) Remote Workers
https://hbr.org/2020/03/a-guide-to-managing-your-newly-remote-workers

F. Smartsheet.com

1. Infrastructure Management 101: A Beginner's Guide to IT Infrastructure Management

https://www.smartsheet.com/it-infrastructure-management-services-guide

G. Simplicable.com

For FAQs / Glossary: https://simplicable.com/new/information-technology